ENCIPHERING SYSTEM, DECIPHERING SYSTEM, INFORMATION CONCEALMENT PROCESSING SYSTEM AND INFORMATION-CONCEALED COMMUNICATION SYSTEM

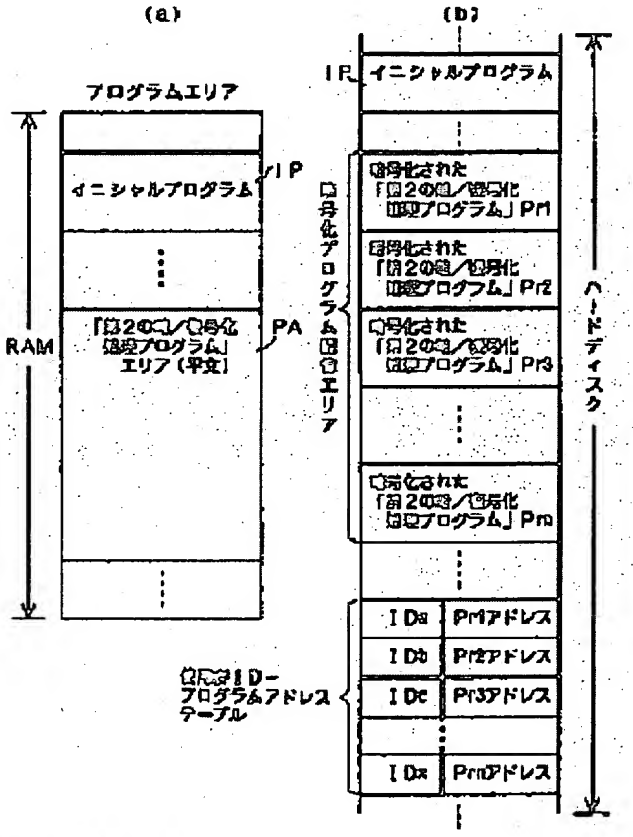
Patent number: JP9006232
Publication date: 1997-01-10
Inventor: SAKA YASUHIKO
Applicant: RICOH ELEMEX CORP;; RICOH CO LTD
Classification:
- international: G09C1/00; G06F9/06; H04L9/00; H04L9/10; H04L9/12
- european:
Application number: JP19950154513 19950621
Priority number(s):

Report a data error here

Abstract of **JP9006232**

PURPOSE: To provide a system which enables ciphering and deciphering to be carried out with efficiency without a program being falsified.

CONSTITUTION: Enciphered enciphering/deciphering processing programs Pr1, Pr2,... are transmitted from an information processing device to an IC card by an initial program IP when a password agrees, the IC card deciphers these programs with a deciphering key of a rightful user and sends them back. An information processing device disposes these programs in a work memory area PA, causes them to get started and carried out data enciphering/deciphering processing. Accordingly, these programs, being normally in an enciphered condition, are neither analized nor falsified by a third party. After the rightful user has completed data processing, the deciphered plain programs are erased so as not to leave room for the plain programs surviving after the processing, and security of these programs is thereby assured. Enciphering work can be carried out with efficiency without a need for work of taking a storage medium of these programs out of a deposit place and setting it in the information processing device.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－6232

(43)公開日　平成９年(1997)１月10日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０９Ｃ	1/00		7259－5Ｊ	Ｇ０９Ｃ	1/00	
Ｇ０６Ｆ	9/06	５５０		Ｇ０６Ｆ	9/06	５５０Ａ
Ｈ０４Ｌ	9/00			Ｈ０４Ｌ	9/00	Ｚ
	9/10					
	9/12					

審査請求　未請求　請求項の数21　ＯＬ　（全 20 頁）

(21)出願番号　特願平7－154513

(22)出願日　平成７年(1995)６月21日

(71)出願人　000006932
リコーエレメックス株式会社
名古屋市中区錦二丁目２番13号

(71)出願人　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号

(72)発明者　坂　康彦
愛知県名古屋市東区泉２丁目28番24号　リコーエレメックス株式会社内

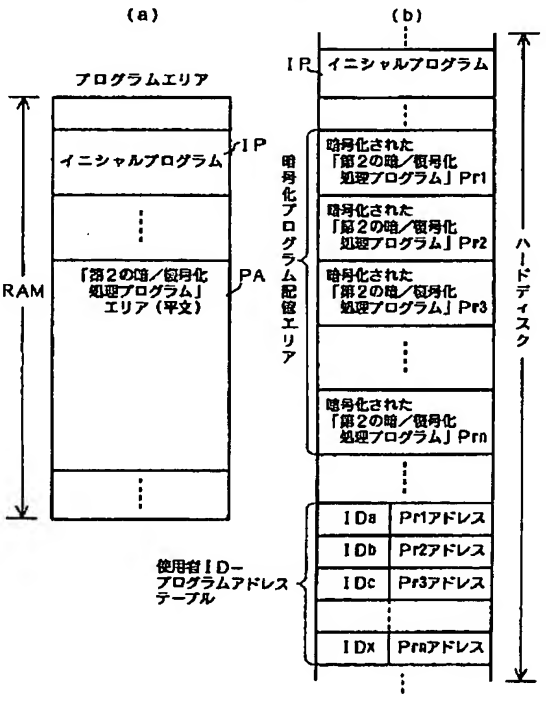
(74)代理人　弁理士　足立　勉

(54)【発明の名称】　暗号化システム、復号化システム、情報秘匿処理システムおよび情報秘匿通信システム

(57)【要約】

【目的】　ﾌﾟﾛｸﾞﾗﾑが改竄されることなく暗号化・復号化を効率的に行うことができるｼｽﾃﾑを提供すること。

【構成】　ｲﾆｼｬﾙﾌﾟﾛｸﾞﾗﾑIPにより、ﾊﾟｽﾜｰﾄﾞが合致すると情報処理装置からICｶｰﾄﾞへ暗号化された暗／復号化処理ﾌﾟﾛｸﾞﾗﾑPr1,Pr2,…が送信され、ICｶｰﾄﾞはこのﾌﾟﾛｸﾞﾗﾑを正当使用者の復号化鍵にて復号化し送り返す。情報処理装置はこのﾌﾟﾛｸﾞﾗﾑを作業ﾒﾓﾘ領域PAに配置して起動しﾃﾞｰﾀの暗／復号化処理を行う。従って通常、ﾌﾟﾛｸﾞﾗﾑは暗号化されているので第三者により解析されず改竄もできない。正当使用者がﾃﾞｰﾀの処理を完了した後はその平文のﾌﾟﾛｸﾞﾗﾑは消去されるため、処理後も平文のﾌﾟﾛｸﾞﾗﾑは残っていず、ﾌﾟﾛｸﾞﾗﾑの安全性が確保される。このため暗号化／復号化処理毎にﾌﾟﾛｸﾞﾗﾑの記憶媒体を保管場所から取り出して情報処理装置にｾｯﾄする作業をしなくても良く効率的に暗号化作業ができる。



【特許請求の範囲】
【請求項１】プログラムに基づく暗号化処理によりデータを暗号化する暗号化システムにおいて、
前記プログラムを、使用者に対応する第１暗号化鍵により暗号化した状態で記憶するプログラム暗号化記憶手段と、
前記プログラム暗号化記憶手段内から、使用者に対応する第１暗号化鍵にて暗号化された前記プログラムを読み出すプログラム読出手段と、
前記プログラム読出手段により読み出された前記プログラムを、使用者に対応する復号化鍵により復号化するプログラム復号化手段と、
前記プログラム復号化手段により復号化されたプログラムを起動させることにより、暗号化対象データを第２暗号化鍵にて暗号化させて暗号化データとするプログラム起動手段と、
前記プログラム起動手段にて暗号化対象データの暗号化が完了すると、復号されて起動対象となった前記プログラムを消去するプログラム消去手段と、
を備えたことを特徴とする暗号化システム。
【請求項２】更に、
前記第２暗号化鍵を、第３暗号化鍵にて暗号化する鍵暗号化手段と、
前記鍵暗号化手段にて暗号化された前記第２暗号化鍵を、前記暗号化データに付加する鍵付加手段と、
を備えた請求項１記載の暗号化システム。
【請求項３】前記鍵付加手段が、前記プログラムの機能として実現されている請求項２記載の暗号化システム。
【請求項４】前記プログラムが、第２暗号化鍵を演算にて求める請求項１～３のいずれかに記載の暗号化システム。
【請求項５】本体装置と、この本体装置とは別体に構成され前記本体装置に対して信号的に任意に接続したり切断したりすることが可能な付属装置とからなり、
前記本体装置が、前記プログラム暗号化記憶手段、前記プログラム読出手段、前記プログラム起動手段、および前記プログラム消去手段を備え、
前記付属装置が、前記使用者に対応する復号化鍵を記憶するとともに、前記プログラム復号化手段を備える請求項１記載の暗号化システム。
【請求項６】本体装置と、この本体装置とは別体に構成され前記本体装置に対して信号的に任意に接続したり切断したりすることが可能な付属装置とからなり、
前記本体装置が、前記プログラム暗号化記憶手段、前記プログラム読出手段、前記プログラム復号化手段、前記プログラム起動手段、および前記プログラム消去手段を備え、
前記付属装置が、前記第３暗号化鍵を記憶するとともに、前記鍵暗号化手段を備える請求項３記載の暗号化システム。
【請求項７】本体装置と、この本体装置とは別体に構成され前記本体装置に対して信号的に任意に接続したり切断したりすることが可能な付属装置とからなり、
前記本体装置が、前記プログラム暗号化記憶手段、前記プログラム読出手段、前記プログラム起動手段、および前記プログラム消去手段を備え、
前記付属装置が、前記使用者に対応する復号化鍵および前記第３暗号化鍵を記憶するとともに、前記プログラム復号化手段および前記鍵暗号化手段を備える請求項３記載の暗号化システム。
【請求項８】前記付属装置が、前記第３暗号化鍵を、復号化を許可する者の管理コードと対応したリストとして記憶する請求項６または７記載の暗号化システム。
【請求項９】前記付属装置が、前記復号化鍵または前記第３暗号化鍵を直接記憶せず、前記復号化鍵または前記第３暗号化鍵が必要とされた場合に、対応する管理コードを用いた演算にて、前記復号化鍵または前記第３暗号化鍵を生成する請求項５～７のいずれかに記載の暗号化システム。
【請求項１０】前記プログラムが、所定時間以内に使用者により次の入力操作が行われない場合に、自己の処理を中止して、前記プログラム消去手段の処理を実行させる機能を有する請求項１～９記載の暗号化システム。
【請求項１１】プログラムに基づく復号化処理により暗号化データを復号化する復号化システムにおいて、
前記プログラムを、使用者に対応する第１暗号化鍵により暗号化した状態で記憶するプログラム暗号化記憶手段と、
前記プログラム暗号化記憶手段内から、使用者に対応する第１暗号化鍵にて暗号化された前記プログラムを読み出すプログラム読出手段と、
前記プログラム読出手段により読み出された前記プログラムを、使用者に対応する復号化鍵により復号化するプログラム復号化手段と、
前記プログラム復号化手段により復号化された前記プログラムを起動させることにより、暗号化データを第２復号化鍵にて復号化させて復号化データとするプログラム起動手段と、
前記プログラム起動手段にて暗号化データの復号化が完了すると、復号化されて起動対象となった前記プログラムを消去するプログラム消去手段と、
を備えたことを特徴とする復号化システム。
【請求項１２】更に、
前記暗号化データに含まれる暗号化された第２復号化鍵を、使用者に対応する復号化鍵にて復号化する鍵復号化手段を備えた請求項１１記載の復号化システム。
【請求項１３】本体装置と、この本体装置とは別体に構成され前記本体装置に対して信号的に任意に接続したり切断したりすることが可能な付属装置とからなり、
前記本体装置が、前記プログラム暗号化記憶手段、前記

プログラム読出手段、前記プログラム起動手段、および前記プログラム消去手段を備え、
前記付属装置が、前記使用者に対応する復号化鍵を記憶するとともに、前記プログラム復号化手段を備える請求項１１記載の復号化システム。
【請求項１４】本体装置と、この本体装置とは別体に構成され前記本体装置に対して信号的に任意に接続したり切断したりすることが可能な付属装置とからなり、
前記本体装置が、前記プログラム暗号化記憶手段、前記プログラム読出手段、前記プログラム復号化手段、前記プログラム起動手段、および前記プログラム消去手段を備え、
前記付属装置が、前記使用者に対応する復号化鍵を記憶するとともに、前記鍵復号化手段を備える請求項１２記載の復号化システム。
【請求項１５】本体装置と、この本体装置とは別体に構成され前記本体装置に対して信号的に任意に接続したり切断したりすることが可能な付属装置とからなり、
前記本体装置が、前記プログラム暗号化記憶手段、前記プログラム読出手段、前記プログラム起動手段、および前記プログラム消去手段を備え、
前記付属装置が、前記使用者に対応する復号化鍵を記憶するとともに、前記プログラム復号化手段および前記鍵復号化手段を備える請求項１２記載の復号化システム。
【請求項１６】前記付属装置が、前記復号化鍵を直接記憶せず、前記復号化鍵が必要とされた場合に、対応する管理コードを用いた演算にて、前記復号化鍵を生成する請求項１３～１５のいずれかに記載の復号化システム。
【請求項１７】前記プログラムが、所定時間以内に使用者により次の入力操作が行われない場合に、自己の処理を中止して、前記プログラム消去手段の処理を実行させる機能を有する請求項１１～１６記載の復号化システム。
【請求項１８】請求項１～１０のいずれか記載の暗号化システムと請求項１１～１７記載の復号化システムとが組合わされてなる情報秘匿処理システム。
【請求項１９】前記暗号化データを通信回線を介して相手方に送信する送信手段を備える請求項１～１０のいずれか記載の暗号化システム。
【請求項２０】前記暗号化データを通信回線を介して受信する受信手段を備える請求項１１～１７のいずれか記載の復号化システム。
【請求項２１】請求項１９記載の暗号化システムと請求項２０記載の復号化システムとが組合わされてなる情報秘匿通信システム。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】本発明は、プログラムに基づく暗号化処理によりデータを暗号化する暗号化システム、プログラムに基づく復号化処理により暗号化データを復号化する復号化システム、更にこれらの機能を有する情報秘匿処理システムおよび情報秘匿通信システムに関する。
【０００２】
【従来の技術】従来、情報（「データ」とも言う。）内容を秘匿するための手法として、暗号化鍵を用いて秘匿したい情報を暗号化する処理が知られている。情報が一旦暗号化されると、同一の暗号化鍵あるいは特定の復号化鍵を用いないと人間が解読できる状態に戻すことはできないため、そのような暗号化鍵や復号化鍵を有していない他人にとってはその情報の内容を秘密にすることができる。
【０００３】しかし、暗号化鍵や復号化鍵（以下、「暗／復号化鍵」として表す。）が漏洩すれば、たちまち他人に情報が解読されてしまうことから、この暗／復号化鍵に対しても、別の暗号化鍵にて暗号化して保管することにより安全性を高めるファイルセキュリティシステムが提案されている（特開平６－１０２８２２号公報）。
【０００４】
【発明が解決しようとする課題】しかし、このようなシステムにおいても、次のような問題が存在した。すなわち、情報の暗号化処理あるいは情報解読のための復号化処理は、一般的には、コンピュータシステムを用いた情報処理装置にて、暗号化プログラムあるいは復号化プログラム（以下、「暗号化・復号化プログラム」として表す）によりなされるのが普通である。
【０００５】この暗号化・復号化プログラムにより、情報が暗号化され、更に安全性を高めるために、その暗／復号化鍵まで暗号化した場合、一見、その情報自体は極めて安全であるように考えられる。ところが、この暗号化・復号化を行う暗号化・復号化プログラム自体は、情報自体よりも無防備であることが多い。もし、この暗号化・復号化プログラムのアルゴリズムが第三者により解析されると、暗号化された情報の解読に利用される恐れがある。
【０００６】また、第三者が、その暗号化・復号化プログラム自体を、正当な使用者に解らないように改竄し、第三者が知っている暗号化鍵にて暗号化する機能を付加することにより、その後、暗号化された情報をすべて第三者が解読してしまう恐れもある。更に、暗号化・復号化プログラム内に、暗号化する前の平文状態（暗号化されていない状態を言う。）の情報を第三者が管理する領域にもコピーしてしまう機能を付加する恐れもあった。
【０００７】勿論、暗号化・復号化プログラムを使用しない場合には、暗号化・復号化プログラムを厳重に保管することも考えられるが、使用毎に、フロッピー等を保管場所から取り出して、情報処理装置にセットして暗号化・復号化プログラムをロードする処理を行わなくてはならず、暗号化・復号化処理が効率的に行うことができない。

【０００８】本発明は、第三者に改竄されることなく、かつ暗号化・復号化を効率的に行うことができる暗号化システム、復号化システム、情報秘匿処理システムおよび情報秘匿通信システムを提供することを目的とする。

【０００９】

【課題を解決するための手段】請求項１記載の発明は、プログラムに基づく暗号化処理によりデータを暗号化する暗号化システムにおいて、前記プログラムを、使用者に対応する第１暗号化鍵により暗号化した状態で記憶するプログラム暗号化記憶手段と、前記プログラム暗号化記憶手段内から、使用者に対応する第１暗号化鍵にて暗号化された前記プログラムを読み出すプログラム読出手段と、前記プログラム読出手段により読み出された前記プログラムを、使用者に対応する復号化鍵により復号化するプログラム復号化手段と、前記プログラム復号化手段により復号化されたプログラムを起動させることにより、暗号化対象データを第２暗号化鍵にて暗号化させて暗号化データとするプログラム起動手段と、前記プログラム起動手段にて暗号化対象データの暗号化が完了すると、復号されて起動対象となった前記プログラムを消去するプログラム消去手段と、を備えたことを特徴とする暗号化システムである。

【００１０】請求項２記載の発明は、更に、前記第２暗号化鍵を、第３暗号化鍵にて暗号化する鍵暗号化手段と、前記鍵暗号化手段にて暗号化された前記第２暗号化鍵を、前記暗号化データに付加する鍵付加手段と、を備えた請求項１記載の暗号化システムである。

【００１１】請求項３記載の発明は、前記鍵付加手段が、前記プログラムの機能として実現されている請求項２記載の暗号化システムである。請求項４記載の発明は、前記プログラムが、第２暗号化鍵を演算にて求める請求項１～３のいずれかに記載の暗号化システムである。

【００１２】請求項５記載の発明は、本体装置と、この本体装置とは別体に構成され前記本体装置に対して信号的に任意に接続したり切断したりすることが可能な付属装置とからなり、前記本体装置が、前記プログラム暗号化記憶手段、前記プログラム読出手段、前記プログラム起動手段、および前記プログラム消去手段を備え、前記付属装置が、前記使用者に対応する復号化鍵を記憶するとともに、前記プログラム復号化手段を備える請求項１記載の暗号化システムである。

【００１３】請求項６記載の発明は、本体装置と、この本体装置とは別体に構成され前記本体装置に対して信号的に任意に接続したり切断したりすることが可能な付属装置とからなり、前記本体装置が、前記プログラム暗号化記憶手段、前記プログラム読出手段、前記プログラム復号化手段、前記プログラム起動手段、および前記プログラム消去手段を備え、前記付属装置が、前記第３暗号化鍵を記憶するとともに、前記鍵暗号化手段を備える請求項３記載の暗号化システムである。

【００１４】請求項７記載の発明は、本体装置と、この本体装置とは別体に構成され前記本体装置に対して信号的に任意に接続したり切断したりすることが可能な付属装置とからなり、前記本体装置が、前記プログラム暗号化記憶手段、前記プログラム読出手段、前記プログラム起動手段、および前記プログラム消去手段を備え、前記付属装置が、前記使用者に対応する復号化鍵および前記第３暗号化鍵を記憶するとともに、前記プログラム復号化手段および前記鍵暗号化手段を備える請求項３記載の暗号化システムである。

【００１５】請求項８記載の発明は、前記付属装置が、前記第３暗号化鍵を、復号化を許可する者の管理コードと対応したリストとして記憶する請求項６または７記載の暗号化システムである。請求項９記載の発明は、前記付属装置が、前記復号化鍵または前記第３暗号化鍵を直接記憶せず、前記復号化鍵または前記第３暗号化鍵が必要とされた場合に、対応する管理コードを用いた演算にて、前記復号化鍵または前記第３暗号化鍵を生成する請求項５～７のいずれかに記載の暗号化システムである。

【００１６】請求項１０記載の発明は、前記プログラムが、所定時間以内に使用者により次の入力操作が行われない場合に、自己の処理を中止して、前記プログラム消去手段の処理を実行させる機能を有する請求項１～９記載の暗号化システムである。

【００１７】請求項１１記載の発明は、プログラムに基づく復号化処理により暗号化データを復号化する復号化システムにおいて、前記プログラムを、使用者に対応する第１暗号化鍵により暗号化した状態で記憶するプログラム暗号化記憶手段と、前記プログラム暗号化記憶手段内から、使用者に対応する第１暗号化鍵にて暗号化された前記プログラムを読み出すプログラム読出手段と、前記プログラム読出手段により読み出された前記プログラムを、使用者に対応する復号化鍵により復号化するプログラム復号化手段と、前記プログラム復号化手段により復号化された前記プログラムを起動させることにより、暗号化データを第２復号化鍵にて復号化させて復号化データとするプログラム起動手段と、前記プログラム起動手段にて暗号化データの復号化が完了すると、復号化されて起動対象となった前記プログラムを消去するプログラム消去手段と、を備えたことを特徴とする復号化システムである。

【００１８】請求項１２記載の発明は、更に、前記暗号化データに含まれる暗号化された第２復号化鍵を、使用者に対応する復号化鍵にて復号化する鍵復号化手段を備えた請求項１１記載の復号化システムである。

【００１９】請求項１３記載の発明は、本体装置と、この本体装置とは別体に構成され前記本体装置に対して信号的に任意に接続したり切断したりすることが可能な付属装置とからなり、前記本体装置が、前記プログラム暗

号化記憶手段、前記プログラム読出手段、前記プログラム起動手段、および前記プログラム消去手段を備え、前記付属装置が、前記使用者に対応する復号化鍵を記憶するとともに、前記プログラム復号化手段を備える請求項１１記載の復号化システムである。

【００２０】請求項１４記載の発明は、本体装置と、この本体装置とは別体に構成され前記本体装置に対して信号的に任意に接続したり切断したりすることが可能な付属装置とからなり、前記本体装置が、前記プログラム暗号化記憶手段、前記プログラム読出手段、前記プログラム復号化手段、前記プログラム起動手段、および前記プログラム消去手段を備え、前記付属装置が、前記使用者に対応する復号化鍵を記憶するとともに、前記鍵復号化手段を備える請求項１２記載の復号化システムである。

【００２１】請求項１５記載の発明は、本体装置と、この本体装置とは別体に構成され前記本体装置に対して信号的に任意に接続したり切断したりすることが可能な付属装置とからなり、前記本体装置が、前記プログラム暗号化記憶手段、前記プログラム読出手段、前記プログラム起動手段、および前記プログラム消去手段を備え、前記付属装置が、前記使用者に対応する復号化鍵を記憶するとともに、前記プログラム復号化手段および前記鍵復号化手段を備える請求項１２記載の復号化システムである。

【００２２】請求項１６記載の発明は、前記付属装置が、前記復号化鍵を直接記憶せず、前記復号化鍵が必要とされた場合に、対応する管理コードを用いた演算にて、前記復号化鍵を生成する請求項１３～１５のいずれかに記載の復号化システムである。

【００２３】請求項１７記載の発明は、前記プログラムが、所定時間以内に使用者により次の入力操作が行われない場合に、自己の処理を中止して、前記プログラム消去手段の処理を実行させる機能を有する請求項１１～１６記載の復号化システムである。

【００２４】請求項１８記載の発明は、請求項１～１０のいずれか記載の暗号化システムと請求項１１～１７記載の復号化システムとが組合わされてなる情報秘匿処理システムである。請求項１９記載の発明は、前記暗号化データを通信回線を介して相手方に送信する送信手段を備える請求項１～１０のいずれか記載の暗号化システムである。

【００２５】請求項２０記載の発明は、前記暗号化データを通信回線を介して受信する受信手段を備える請求項１１～１７のいずれか記載の復号化システムである。請求項２１記載の発明は、請求項１９記載の暗号化システムと請求項２０記載の復号化システムとが組合わされてなる情報秘匿通信システムである。

【００２６】

【作用及び発明の効果】請求項１の暗号化システムは、プログラム暗号化記憶手段、プログラム読出手段、プログラム復号化手段、プログラム起動手段およびプログラム消去手段を備え、プログラム暗号化記憶手段は、暗号化処理用のプログラムを、使用者に対応する第１暗号化鍵により暗号化した状態で記憶する。プログラム読出手段は、前記プログラム暗号化記憶手段内から、使用者に対応する第１暗号化鍵にて暗号化された前記プログラムを読み出す。プログラム復号化手段は、前記プログラム読出手段により読み出された前記プログラムを、使用者に対応する復号化鍵により復号化する。プログラム起動手段は、前記プログラム復号化手段により復号化されたプログラムを起動させることにより、暗号化対象データを第２暗号化鍵にて暗号化させて暗号化データとする。プログラム消去手段は、前記プログラム起動手段にて暗号化対象データの暗号化が完了すると、復号されて起動対象となった前記プログラムを消去する。

【００２７】このように、本発明の暗号化システムにて起動する暗号化処理用のプログラムは、暗号化処理に用いられていない場合には、プログラム暗号化記憶手段により暗号化された状態で記憶されている。したがって、暗号化されたままでは、第三者により、解析されることはなく、また解析できないので改竄もできない。また、復号化鍵は使用者が所持することにより、第三者にプログラム復号化手段が判明しても暗号化処理用のプログラムを復号化することはできない。

【００２８】正当な使用者がデータを暗号化する場合には、プログラム読出手段が、プログラム暗号化記憶手段内から、使用者に対応する第１暗号化鍵にて暗号化された前記プログラムを読み出し、プログラム復号化手段が、そのプログラムを、使用者に対応する復号化鍵により復号化し、プログラム起動手段が、その復号化されたプログラムを起動させる。この起動された前記プログラムの機能により、暗号化対象データが第２暗号化鍵にて暗号化されて暗号化データとなる。

【００２９】しかも、データの暗号化が完了した後は、プログラム消去手段が、その起動された平文状態のプログラムを消去する。このため、暗号化処理をした後も、平文状態の暗号化用のプログラムが残っていることがなく、暗号化用のプログラムの安全性が確保され、結果として、暗号化されたデータの安全性も確保される。したがって、暗号化処理毎に、暗号化処理用のプログラムを記憶している記憶媒体を保管場所から取り出してコンピュータにセットしてロードする作業をしなくても良く、効率的に暗号化作業ができる。

【００３０】上記構成に更に、鍵暗号化手段および鍵付加手段を加えても良い。この鍵暗号化手段は、前記第２暗号化鍵を、第３暗号化鍵にて暗号化する。そして、鍵付加手段は、前記鍵暗号化手段にて暗号化された前記第２暗号化鍵を、前記暗号化データに付加する。

【００３１】このように、データを暗号化するための第２暗号化鍵を、更に第３暗号化鍵にて暗号化しているの

で、鍵付加手段にて、暗号化データに第２暗号化鍵を付加しておいても安全は確保できる。また、暗号化データに第２暗号化鍵が付加されるので、その記憶媒体のまま持ち運んだり、あるいはその暗号化データを通信により相手方に送信しても、持ち運び先あるいは通信相手先にて、第３暗号化鍵さえ保管されていれば、暗号化データを復号化することができる。すなわち、暗号化データに付加されている暗号化された第２暗号化鍵を第３暗号化鍵にて復号化し、次に復号化された第２暗号化鍵にて、暗号化データを復号化することができる。尚、鍵付加手段は、前記暗号化用のプログラムの機能として実現されていても良い。

【００３２】更に、この場合、第２暗号化鍵が、前記暗号化用のプログラムにより演算にて求められたものであっても良い。このように演算にて求められる暗号化鍵は一時的な鍵であり、継続して使用されるものではないので、よりデータの安全性が確保される。また、この一時的な鍵も、上記暗号化用のプログラムにて演算されていることから、暗号化処理時以外は、その第２暗号化鍵を生成するプログラムは暗号化されたもののみが存在しているので、第三者が知っている鍵を生成するように改竄することはできない。

【００３３】また、本暗号化システムは、本体装置と、この本体装置とは別体に構成され前記本体装置に対して信号的に任意に接続したり切断したりすることが可能な付属装置とに別れて構成されていても良い。例えば、本体装置を、コンピュータ装置とし、付属装置を、ＩＣカードとする構成が挙げられる。

【００３４】この場合、本体装置が、前記プログラム暗号化記憶手段、前記プログラム読出手段、前記プログラム起動手段、および前記プログラム消去手段を備え、付属装置が、前記使用者に対応する復号化鍵を記憶するとともに、前記プログラム復号化手段を備える構成としても良い。

【００３５】このように構成すると、暗号化処理をしない場合には、本体装置から付属装置を切り離して、安全な保管場所に収納しておくことができる。付属装置側には、使用者に対応する復号化鍵とプログラム復号化手段とが存在するため、その復号化鍵およびプログラム復号化手段のプログラムの安全性が共に確保され、データの安全性が一層確保される。

【００３６】また、同様に、本体装置と付属装置とに別々に構成された場合に、本体装置が、前記プログラム暗号化記憶手段、前記プログラム読出手段、前記プログラム復号化手段、前記プログラム起動手段、および前記プログラム消去手段を備え、付属装置が、前記第３暗号化鍵を記憶するとともに、前記鍵暗号化手段を備える構成としても良い。

【００３７】このように構成すると、付属装置側には、第３暗号化鍵と鍵暗号化手段とが存在するため、その第３暗号化鍵および鍵暗号化手段のプログラムの安全性が共に確保され、データの安全性が一層確保される。また、本体装置と付属装置とに別々に構成された場合に、上記両者を加味した構成、すなわち、本体装置が、前記プログラム暗号化記憶手段、前記プログラム読出手段、前記プログラム起動手段、および前記プログラム消去手段を備え、付属装置が、前記使用者に対応する復号化鍵および前記第３暗号化鍵を記憶するとともに、前記プログラム復号化手段および前記鍵暗号化手段を備える構成としても良い。

【００３８】このように構成すると、付属装置側には、使用者に対応する復号化鍵、第３暗号化鍵、プログラム復号化手段および鍵暗号化手段とが存在するため、その使用者に対応する復号化鍵、第３暗号化鍵、プログラム復号化手段のプログラムおよび鍵暗号化手段のプログラムの安全性がすべて確保され、データの安全性が一層確保される。

【００３９】また、前記付属装置が、第３暗号化鍵を、復号化を許可する者の管理コードと対応したリストとして記憶していても良い。このように構成されていると、管理コード、例えばＩＤにて復号化を許可する者を指定すれば、付属装置の鍵暗号化手段がそのＩＤに対応した第３暗号化鍵にて第２暗号化鍵を暗号化することができる。

【００４０】また、前記付属装置が、復号化鍵または第３暗号化鍵を直接記憶せず、復号化鍵または第３暗号化鍵が必要とされた場合に、対応する管理コードを用いた演算にて、復号化鍵または第３暗号化鍵を生成するものとしても良い。特に、第３暗号化鍵が多数記憶しなくてはならない場合に、演算式のみで良いのでメモリの節約となる。

【００４１】また前記プログラムが、所定時間以内に使用者により次の入力操作が行われない場合に、自己の処理を中止して、前記プログラム消去手段の処理を実行させる機能を有するものとしても良い。このようにすれば、正当な使用者がシステム装置から一旦離れたとしても、しばらくすると平文状態のプログラム自体が消え去るので第三者に解析されたり改竄されたりすることがない。

【００４２】請求項１１の復号化システムは、プログラム暗号化記憶手段、プログラム読出手段、プログラム復号化手段、プログラム起動手段およびプログラム消去手段とを備え、プログラム暗号化記憶手段は、前記プログラムを、使用者に対応する第１暗号化鍵により暗号化した状態で記憶し、プログラム読出手段は、前記プログラム暗号化記憶手段内から、使用者に対応する第１暗号化鍵にて暗号化された前記プログラムを読み出し、プログラム復号化手段は、前記プログラム読出手段により読み出された前記プログラムを、使用者に対応する復号化鍵により復号化し、プログラム起動手段は、前記プログラ

ム復号化手段により復号化された前記プログラムを起動させることにより、暗号化データを第２復号化鍵にて復号化させて復号化データとし、プログラム消去手段は、前記プログラム起動手段にて暗号化データの復号化が完了すると、復号化されて起動対象となった前記プログラムを消去する。

【００４３】このように、本発明の復号化システムにて起動する復号化処理用のプログラムは、復号化処理に用いられていない場合には、プログラム暗号化記憶手段により暗号化された状態で記憶されている。したがって、暗号化されたままでは、第三者により、解析されることはなく、また解析できないので改竄もできない。また、復号化鍵は使用者が所持することにより、第三者にプログラム復号化手段が判明しても復号化処理用のプログラムを復号化することはできない。

【００４４】正当な使用者が暗号化データを復号化する場合には、プログラム読出手段が、プログラム暗号化記憶手段内から、使用者に対応する第１暗号化鍵にて暗号化された前記プログラムを読み出し、プログラム復号化手段が、そのプログラムを、使用者に対応する復号化鍵により復号化し、プログラム起動手段が、その復号化されたプログラムを起動させる。この起動された前記プログラムの機能により、暗号化データを第２復号化鍵にて復号化させて復号化データ、すなわち平文データとすることができる。

【００４５】しかも、暗号化データの復号化が完了した後は、プログラム消去手段が、その起動された平文状態のプログラムを消去する。このため、復号化処理をした後も、平文状態の復号化用のプログラムが残っていることもなく、復号化用のプログラムの安全性が確保され、結果として、データの安全性も確保される。したがって、復号化処理毎に、復号化処理用のプログラムを記憶している記憶媒体を保管場所から取り出してコンピュータにセットしてロードする作業をしなくても良く、効率的に復号化作業ができる。

【００４６】上記構成に更に、鍵復号化手段をを加えても良い。この鍵復号化手段は、暗号化データに含まれる暗号化された第２復号化鍵を、使用者に対応する復号化鍵にて復号化する。このようにすることにより、暗号化データを復号化するための第２復号化鍵が得られ、正当な使用者のみが適切に暗号化データを復号化して平文データを得ることができる。

【００４７】また、本復号化システムは、本体装置と、この本体装置とは別体に構成され前記本体装置に対して信号的に任意に接続したり切断したりすることが可能な付属装置とに別れて構成されていても良い。例えば、本体装置を、コンピュータ装置とし、付属装置を、ＩＣカードとする構成が挙げられる。

【００４８】この場合、本体装置が、前記プログラム暗号化記憶手段、前記プログラム読出手段、前記プログラム起動手段、および前記プログラム消去手段を備え、付属装置が、前記使用者に対応する復号化鍵を記憶するとともに、前記プログラム復号化手段を備える構成としても良い。

【００４９】このように構成すると、復号化処理をしない場合には、本体装置から付属装置を切り離して、安全な保管場所に収納しておくことができる。付属装置側には、使用者に対応する復号化鍵とプログラム復号化手段とが存在するため、その復号化鍵およびプログラム復号化手段のプログラムの安全性が共に確保され、データの安全性が一層確保される。

【００５０】また、同様に、本体装置と付属装置とに別々に構成された場合に、本体装置が、前記プログラム暗号化記憶手段、前記プログラム読出手段、前記プログラム復号化手段、前記プログラム起動手段、および前記プログラム消去手段を備え、付属装置が、使用者に対応する復号化鍵を記憶するとともに、前記鍵復号化手段を備える構成としても良い。

【００５１】このように構成すると、付属装置側には、使用者に対応する復号化鍵と鍵復号化手段とが存在するため、その復号化鍵および鍵復号化手段のプログラムの安全性が共に確保され、データの安全性が一層確保される。また、本体装置と付属装置とに別々に構成された場合に、上記両者を加味した構成、すなわち、本体装置が、前記プログラム暗号化記憶手段、前記プログラム読出手段、前記プログラム起動手段、および前記プログラム消去手段を備え、付属装置が、前記使用者に対応する復号化鍵を記憶するとともに、前記プログラム復号化手段および前記鍵復号化手段を備える構成としても良い。

【００５２】このように構成すると、付属装置側には、使用者に対応する復号化鍵、プログラム復号化手段および鍵復号化手段とが存在するため、その使用者に対応する復号化鍵、プログラム復号化手段のプログラムおよび鍵復号化手段のプログラムの安全性がすべて確保され、データの安全性が一層確保される。

【００５３】また、前記付属装置が、復号化鍵を直接記憶せず、復号化鍵が必要とされた場合に、対応する管理コードを用いた演算にて、復号化鍵を生成するものとしても良い。また前記プログラムが、所定時間以内に使用者により次の入力操作が行われない場合に、自己の処理を中止して、前記プログラム消去手段の処理を実行させる機能を有するものとしても良い。このようにすれば、正当な使用者がシステム装置から一旦離れたとしても、しばらくすると平文状態のプログラム自体が消え去るので第三者に解析されたり改竄されたりすることがない。

【００５４】また、上述したいずれかの構成の暗号化システムと上述したいずれかの復号化システムとを組合わせて、情報秘匿処理システムとして構成しても良い。このことにより、一つの情報秘匿処理システムにて、暗号化システムと復号化システムとの両方の機能を有するこ

とができ、使用者の処理が効率的となるとともに、プログラムやデータの安全性も確保される。

【００５５】尚、上述した暗号化システムにおいて、暗号化データを通信回線を介して相手方に送信する送信手段を備えて、例えば暗号化機能を有するファクシミリ装置等のデータ通信システムとして構成することができる。また、上述した復号化システムにおいても同様に、暗号化データを通信回線を介して受信する受信手段を備えて、例えば暗号化データの解読機能を有するファクシミリ装置等のデータ通信システムとして構成することができる。

【００５６】勿論、上述の送信手段を有する暗号化システムと上述の受信手段を有する復号化システムとを組合わせ、暗号化機能および暗号化データ解読機能を有するファクシミリ装置等の情報秘匿通信システムとして構成することができる。

【００５７】

【実施例】図１および図２は、本発明の情報秘匿処理システムの一実施例を示している。この内、図１は、情報処理装置２のブロック図を示す。情報処理装置２は、ＣＰＵ４、ＲＯＭ６、ＲＡＭ８、バックアップＲＡＭ１０、キーボード１２、光磁気ディスク（ＭＯＤ）ドライブ１４、ＣＲＴディスプレイ１６、ハードディスク（ＨＤ）装置１８、フロッピーディスク（ＦＤ）ドライブ２０および入出力インターフェイス（Ｉ／Ｏ）２２を備えている。これらの構成はバス２４にて信号的に接続され、更にＩ／Ｏ２２にはＩＣカードリーダー２６が接続されている。

【００５８】このように、情報処理装置２はコンピュータとして構成され、ＲＯＭ６、光磁気ディスクドライブ１４に挿入された光磁気ディスク、ハードディスク装置１８、フロッピーディスクドライブ２０に挿入されたフロッピーディスクあるいはＩＣカードリーダー２６に挿入されたＩＣカード３０（図２）から読み込まれたプログラムやデータに基づいて、必要な処理を実行し、結果として得られたデータを、光磁気ディスクドライブ１４に挿入された光磁気ディスク、ハードディスク装置１８、フロッピーディスクドライブ２０に挿入されたフロッピーディスクあるいはＩＣカードリーダー２６に挿入されたＩＣカード３０に記憶する。情報処理装置２は、これ以外にＣＤ－ＲＯＭドライブ装置や磁気テープ記憶装置等を備えても良い。

【００５９】図２にＩＣカード３０のブロック図を示す。ＩＣカード３０は、ＣＰＵ３２、ＲＯＭ３４、ＲＡＭ３６、バックアップＲＡＭ３８および入出力インターフェイス（Ｉ／Ｏ）４０を備えている。これらの構成はバス４２にて信号的に接続されている。尚、Ｉ／Ｏ４０は、情報処理装置２のＩＣカードリーダー２６に対するコネクタを備えたインターフェイスである。

【００６０】前記情報処理装置２の電源オンにより、図３（ａ）に示すごとくＲＡＭ８のプログラムエリアに、データを暗号化および復号化するためのイニシャルプログラムＩＰがハードディスク装置１８からロードされて起動される。尚、ハードディスク装置１８には、図３（ｂ）に示すごとく、イニシャルプログラムＩＰ以外に、複数の暗号化された「第２の暗／復号化処理プログラム」Ｐr1～Ｐrnが格納されている。これらの「第２の暗／復号化処理プログラム」Ｐr1～Ｐrnは、本情報処理装置２の使用者の暗号化鍵（第１暗号化鍵）にて暗号化されたものであり、使用者の数だけ存在し、復号化すれば基本的には同じ機能を有しているプログラムである。ただし、後述するごとく使用者毎に異なる機能を持たせることもできる。使用者とプログラムとの対応は、図３（ｂ）に示すハードディスク装置１８内の使用者ＩＤ－プログラムアドレステーブルを参照することにより行われる。これらの「第２の暗／復号化処理プログラム」Ｐr1～Ｐrnおよび使用者ＩＤ－プログラムアドレステーブルは、前記イニシャルプログラムＩＰとともにハードディスク装置１８に予めインストールされている。

【００６１】また、ＩＣカード３０のバックアップＲＡＭ３８には、図４に示すごとく、パスワード照合プログラムＰr11、暗号化処理プログラムＰr12、復号化処理プログラムＰr13、鍵暗号化処理プログラムＰr14および鍵復号化処理プログラムＰr15等のプログラムと、正当な使用者のパスワード、正当な使用者のＩＤ、正当な使用者の暗／復号化鍵（第１暗号化鍵および復号化鍵に該当する）および正当な使用者がデータの復号化を許可する相手のＩＤ（ＩＤ1，ＩＤ2，…，ＩＤn）とそのＩＤに対応する相手方暗号化鍵Ｋ1，Ｋ2，…，Ｋnが記憶されている。

【００６２】使用者が、データを暗号化するために、情報処理装置２を電源オンした場合には、図５および図６のフローチャートに示すイニシャルプログラムＩＰが起動される。まず、ステップＳ１００にて初期化処理が行われ、情報処理装置２に存在する各種構成の初期状態を設定し、プログラムに使用するデータの初期値を決定する等の処理がなされる。

【００６３】次に、ＩＣカードリーダー２６にＩＣカード３０が装着されているか否かが判定される（Ｓ１１０）。装着されていなければステップＳ１１０にては否定判定されて、ＩＣカード３０の装着を要求する表示をＣＲＴディスプレイ１６に行って（Ｓ１２０）、再度ステップＳ１１０を実行する処理を繰り返す。

【００６４】ＩＣカード３０が、ＩＣカードリーダー２６に装着されれば、ステップＳ１１０にて肯定判定されて、次にパスワードを要求する表示がＣＲＴディスプレイ１６になされる（Ｓ１３０）。このパスワードは、図４に示したＩＣカード３０の正当な使用者のパスワードを求めるものである。

【００６５】パスワードの入力がキーボード１２からな

されたか否かが判定され（Ｓ１４０）、入力が無ければ、ステップＳ１５０にてタイムアウトと判定されるまで、ステップＳ１４０，Ｓ１５０の処理を繰り返す。タイムアウトに該当する所定時間経過してもパスワードの入力がなされなければステップＳ１５０にて、肯定判定されて、本イニシャルプログラムの処理を終了する。タイムアウトする前にパスワードの入力があれば、ステップＳ１４０にて肯定判定されて、入力されたパスワードがＩＣカード３０側に送信される。そして、次に、ＩＣカード３０側からパスワードの照合結果とその使用者のＩＤとが送信されて来るのを待つ（Ｓ１７０）。

【００６６】図７～図８のフローチャートにＩＣカード３０側の処理を示す。本処理はＩＣカード３０がＩＣカードリーダー２６に装着された際に起動される処理である。まず、情報処理装置２からのパスワードの受信待ちとなる（Ｓ５００）。前述したステップＳ１６０の処理により、パスワードが送信されて来ればステップＳ５００にて肯定判定されて、パスワード照合プログラムＰｒ11により、図４に示したバックアップＲＡＭ３８に記憶された、このＩＣカード３０の正当な使用者のパスワードと、情報処理装置２から送られたパスワードとの照合がなされる（Ｓ５２０）。

【００６７】そして、その照合の結果と正当な使用者のＩＤとが情報処理装置２側へ送信される（Ｓ５３０）。次に照合結果が「合致」、すなわち、情報処理装置２からのパスワードとバックアップＲＡＭ３８内に記憶されていた正当使用者のパスワードとが一致すれば、正当な使用者がそのＩＣカード３０を使用していることが判るので、次にその正当な使用者の暗／復号化鍵を、バックアップＲＡＭ３８から読み出す（Ｓ５５０）。もし、パスワードの照合結果が不一致となった場合に、ステップＳ５４０にて否定判定されて、再度ステップＳ５００の処理に戻る。

【００６８】ステップＳ５５０を処理した場合には、次に情報処理装置２からの送信待ちとなる（Ｓ５６０）。ステップ５３０の処理にて、照合結果とＩＤとが情報処理装置２へ送信されると、情報処理装置２側では、ステップ１７０にて肯定判定されて、次に合致したか否かが判定される（Ｓ１８０）。合致していなければ、正当な使用者では無いので、ステップ１８０にて否定判定されて、ＣＲＴディスプレイ１６に、不一致であることと処理を中止するとの表示をして（Ｓ１９０）、ステップＳ１１０の処理に戻る。したがって、ＩＣカード３０がＩＣカードリーダー２６に装着されていれば、再度、ステップ１３０にてパスワードが要求され、ステップ１４０，Ｓ１５０にて、パスワード入力待ちとなる。パスワードの入力を間違えても、再度、入力を求められるので正当な使用者ならば訂正すれば良い。しかし、不正な使用である場合には、パスワードを繰り返して入力させるのは一致の可能性が高くなるので、パスワードの入力間違いは例えば３回までとし、ステップＳ１８０にて３回目の間違いの場合には、ステップＳ１１０に戻さず、本イニシャルプログラムを終了するようにする。

【００６９】ステップＳ１８０にて、合致したとの判定がなされると、ＣＲＴディスプレイ１６に合致した旨の表示がなされ（Ｓ２００）、次にＩＣカード３０から照合結果と共に受信したＩＤに対応する暗号化された第２の暗／復号化処理プログラムをハードディスク装置１８の記憶ファイルから探し出して、ＩＣカード３０側へ送信する（Ｓ２１０）。ＩＤからプログラムを探すのは、図３（ｂ）に示したごとく、ハードディスク装置１８にファイルされている使用者ＩＤ－プログラムアドレステーブルから、ＩＤに対応する暗号化された第２の暗／復号化処理プログラムのディスク上のアドレスを得て、そのアドレスから該当する暗号化された第２の暗／復号化処理プログラムを読み出すことにより行われる。例えば、使用者のＩＤがＩＤbであれば、暗号化された第２の暗／復号化処理プログラムPr2が対応していることが、使用者ＩＤ－プログラムアドレステーブルから判明し、そのディスクアドレスから、暗号化された第２の暗／復号化処理プログラムPr2が読み出される。

【００７０】次に、ＩＣカード３０からの送信待ちとなる（Ｓ２２０）。ＩＣカード３０側では、情報処理装置２から暗号化された第２の暗／復号化処理プログラムＰr2の送信があると、ステップＳ５６０の判定にて肯定判定されて、次にそのプログラムＰr2の受信とその受信したプログラムPr2の復号化処理がなされる（Ｓ５７０）。すなわち、バックアップＲＡＭ３８に存在する復号化処理プログラムＰｒ13を起動して、情報処理装置２から送信されて来たプログラムPr2を復号化する。尚、プログラムPr2が長くて、バッファや作業メモリ容量の関係で一度に送信あるいは復号化できない場合には、分割して送信あるいは復号化しても良い。

【００７１】次に、復号化した第２の暗／復号化処理プログラムPr2を情報処理装置２へ送信する（Ｓ５８０）。次に、暗号化していない一時鍵および復号化対象者ＩＤが受信されたか否かが判定され（Ｓ５９０）、受信していなければ、暗号化された一時鍵が受信されたか否かが判定される（Ｓ５９５）。これも受信していなければ、暗号化していない第２の暗／復号化処理プログラムが受信されたか否かが判定される（Ｓ６００）。いずれも受信していない内は、ステップＳ５９０，ステップＳ５９５およびステップＳ６００の判定を繰り返す。

【００７２】情報処理装置２側では、ＩＣカード３０側から、復号化された、すなわち平文の第２の暗／復号化処理プログラムPr2を受信すると、ステップＳ２２０にて肯定判定されて、その平文の第２の暗／復号化処理プログラムPr2を、図２（ａ）に示すごとくＲＡＭ８の作業メモリ領域ＰＡに転送する（Ｓ２３０）。

【００７３】次に、この平文の第２の暗／復号化処理プ

ログラムＰr2がイニシャルプログラムから起動される（Ｓ２４０）。その第２の暗／復号化処理プログラムＰr2のフローチャートを図９～図１２に示す。この処理がステップＳ２４０の起動処理により実行される。

【００７４】第２の暗／復号化処理プログラムＰr2の処理が開始されると、まず、処理メニューがＣＲＴディスプレイ１６に表示される（Ｓ１０１０）。メニューは、暗号化処理（Ｓ１１００）、復号化処理（Ｓ１２００）、第２の暗／復号化処理プログラムの変更処理（Ｓ１３００）およびその他の処理（Ｓ1400）である。

【００７５】ここで、使用者により暗号化処理（Ｓ１１００）が選択されると、図１０に示す処理が開始される。まず、暗号化対象データ名および復号化対象者ＩＤの入力が要求される（Ｓ１１０２）。暗号化対象データ名は、光磁気ディスクドライブ１４にセットされた光磁気ディスク、ハードディスク装置１８あるいはフロッピーディスクドライブ２０にセットされたフロッピーディスク内のファイルを指定することにより行う。ここでは、光磁気ディスクに暗号化データを格納するため、暗号化対象データは、フロッピーディスクに存在するものとする。

【００７６】また復号化対象者ＩＤは、復号化を許可する相手のＩＤを入力する。復号化を許可する相手方が複数であれば複数のＩＤを入力する。尚、予め登録されているグループのＩＤを入力すれば、そのグループに属している複数の相手のＩＤを指定したことになり、一つのＩＤで複数人を復号化対象者とすることができる。

【００７７】ここで、タイムアウト処理（Ｓ１１０６）にて所定のタイムアウト時間が経過するまで、入力待ちとなる（Ｓ１１０４）。タイムアウトまで、入力がなければ、ステップＳ１１０６にて肯定判定されて、直ちにイニシャルプログラムへ帰るが、暗号化対象データ名および復号化対象者ＩＤの入力がなされれば、次に一時鍵（第２暗号化鍵）を生成する（Ｓ１１０８）。

【００７８】ここで、一時鍵の生成は、生成毎に異なる鍵（値や文字列）であることが好ましい。例えば、Ｍ系列乱数発生プログラムによる方法やキー操作の時間間隔を１０万分の１秒程度で測定して下位の必要桁数のみ取り出す方法等が挙げられる。こうして生成された一時鍵と復号化対象者ＩＤとをＩＣカード３０側へ送信し（Ｓ１１１０）、次にＩＣカード３０側から送信されて来る暗号化された一時鍵の受信待ちとなる（Ｓ１１２０）。

【００７９】ＩＣカード３０側では、一時鍵と復号化対象者ＩＤとを受信したので、図８のステップＳ５９０にて肯定判定されて、次に、一時鍵暗号化処理プログラムＰr14により、復号化対象者ＩＤに対応する相手方暗号化鍵により一時鍵を暗号化する（Ｓ６１０）。ＩＣカード３０のバックアップＲＡＭ３８には、図４に示したごとく、正当な使用者がデータの復号化を許可する相手のＩＤ1，ＩＤ2，…，ＩＤnとそのＩＤに対応する相手方暗号化鍵Ｋ1，Ｋ2，…，Knが記憶されていることから、例えば、復号化対象者ＩＤがＩＤ2であれば、対応する相手方暗号化鍵Ｋ2が選択され、その相手方暗号化鍵Ｋ2により一時鍵を暗号化する。また、グループのＩＤが入力されていれば、そのグループの代表となる者のＩＤから相手方暗号化鍵を選択してその相手方暗号化鍵にて一時鍵を暗号化してもよく、またグループ独自の相手方暗号化鍵にて一時鍵を暗号化しても良い。

【００８０】次にこのように暗号化された一時鍵を情報処理装置２側へ送信し（Ｓ６２０）、ＩＣカード３０での処理はステップＳ５００の処理に戻る。情報処理装置２側では、暗号化された一時鍵を受信したので、ステップＳ１１２０にて肯定判定されて、暗号化された一時鍵を、ＩＤとともに記憶媒体にファイルとして格納する（Ｓ１１３０）。この記憶媒体は、使用者が指定する記憶媒体であるが、ここでは、光磁気ディスクドライブ１４にセットされた光磁気ディスクである。勿論、フロッピーディスクあるいはハードディスク装置１８その他の記憶媒体でも良い。

【００８１】次に既にステップＳ１１０２にて入力されている暗号化対象データが読み出され（Ｓ１１４０）、暗号化されていない一時鍵、すなわちステップＳ１１０８で生成されたままの一時鍵により、その暗号化対象データが暗号化される（Ｓ１１５０）。このようなデータを鍵を用いて暗号化処理するプログラムとしては、米国の標準アルゴリズムであるＤＥＳや、ＮＴＴ社が開発したＦＥＥＬ等が知られている。

【００８２】次に、この暗号化されたデータを、ＩＤおよび暗号化された一時鍵が格納されたファイルに格納する（Ｓ１１６０）。すなわち、図１３に示すごとく、ヘッダー部として、復号者（復号を許可する者）のＩＤ(1)，ＩＤ(2)，…，ＩＤ(n)とそのＩＤに対応した暗号化一時鍵Ｋ(1)，Ｋ(2)，…，Ｋ(n)とのリストを記載し、データ部として、一時鍵にて暗号化した暗号化データを記載したファイルとして格納する。

【００８３】こうして、情報処理装置２にて暗号化処理（Ｓ１１００）が終了し、次にＲＡＭ８上に、例えば、ステップＳ１１４０の処理にてＲＡＭ８の作業メモリ領域に読み出されたままの暗号化対象データといった、暗号化されていないデータが存在する場合には、そのデータをクリアする処理（Ｓ１５００）が行われる。

【００８４】こうして、第２の暗／復号化処理が終了し、イニシャルプログラムに戻る。イニシャルプログラムでは、図６に示すステップＳ２５０の処理が行われて、ＲＡＭ８上に存在している第２の暗／復号化処理プログラムをクリアし、ステップＳ１１０の処理に戻る。

【００８５】このようにして、データの暗号化が終了する。上述したごとく、本実施例の情報処理装置２にて起動する暗号化処理用のプログラム（図９，図１０）は、暗号化処理に用いられていない場合には、ハードディス

ク装置１８により暗号化された状態で記憶されている。したがって、第三者により、解析されることはなく、また解析できないので改竄もできない。

【００８６】正当な使用者がデータを暗号化する場合には、ハードディスク装置１８から、正当な使用者の暗／復号化鍵にて暗号化された前記プログラムを読み出し、そのプログラムを、正当な使用者の暗／復号化鍵により復号化し、その復号化されたプログラムを起動させることにより、暗号化対象データを一時鍵（第２暗号化鍵）にて暗号化させて暗号化データとすることができる。

【００８７】しかも、データの暗号化が完了した後は、その起動されたプログラムを消去する。このため、暗号化処理をした後も、平文状態の暗号化用のプログラムが残っていることもなく、暗号化用のプログラムの安全性が確保され、結果として、暗号化されたデータの安全性も確保される。したがって、暗号化処理毎に、暗号化処理用のプログラムを記憶している記憶媒体を保管場所から取り出して情報処理装置２にセットしてロードする作業をしなくても良く、効率的に暗号化作業ができる。

【００８８】また、暗号化前のデータも作業メモリ領域上に残っている場合には、それをクリアしているので、より安全性が高い。更に、一時鍵（第２暗号化鍵）は、相手方暗号化鍵（第３暗号化鍵）にて暗号化される。そして、この暗号化された一時鍵は復号化を許可する者のＩＤとともに、暗号化データと一つのファイルに収納される。

【００８９】このように、データを暗号化するための一時鍵（第２暗号化鍵）を、更に相手方暗号化鍵（第３暗号化鍵）にて暗号化しているので、暗号化データに一時鍵（第２暗号化鍵）を付加しておいても安全は確保できる。また、暗号化データに一時鍵（第２暗号化鍵）が付加されるので、その記憶媒体（ここでは光磁気ディスク）のまま持ち運んだり、あるいはその暗号化データを通信により相手方に送信しても、持ち運び先あるいは通信相手先にて、相手方暗号化鍵（第３暗号化鍵）さえ保管されていれば、暗号化データを復号化することができる。

【００９０】一時鍵（第２暗号化鍵）は、前記暗号化用のプログラムにより演算にて求められたものである。このようにデータを暗号化するための暗号化鍵は、その時の暗号化のためだけの一時的な鍵であり、継続して使用されるものではないので、よりデータの安全性が確保される。また、この一時鍵も、前記暗号化用のプログラム内で演算されていることから、暗号化処理時以外は、そのプログラムは暗号化されたもののみが存在しているので、第三者は自分が知っている鍵を生成するように改竄することはできない。

【００９１】また、本実施例の情報秘匿処理システムは、本体装置としての情報処理装置２と、この情報処理装置２とは別体に構成され情報処理装置２に対して信号的に任意に接続したり切断したりすることが可能な付属装置としてのＩＣカード３０とに別れて構成され、しかも、情報処理装置２が、プログラム暗号化記憶処理、プログラム読出処理、プログラム起動処理、およびプログラム消去処理の各プログラムを備え、ＩＣカード３０が、正当な使用者の暗／復号化鍵および相手方暗号化鍵（第３暗号化鍵）を記憶するとともに、プログラム復号化処理および鍵暗号化処理の各プログラムを備える構成とされている。すなわち、ＩＣカード３０側には、正当な使用者の暗／復号化鍵、相手方暗号化鍵（第３暗号化鍵）、プログラム復号化処理のプログラムおよび鍵暗号化処理のプログラムが存在するため、その正当な使用者の暗／復号化鍵、相手方暗号化鍵（第３暗号化鍵）、プログラム復号化処理のプログラムおよび鍵暗号化処理のプログラムの安全性が確保され、データの安全性が一層確保される。

【００９２】次に、図１３に示した暗号化データファイルを格納した光磁気ディスクを受け取った場合、そのデータを復号化する処理について説明する。使用者は、まず、情報処理装置２の電源オンさせた後、受け取った光磁気ディスクを光磁気ディスクドライブ１４にセットし、自己のＩＣカード３０をＩＣカードリーダー２６にセットする。

【００９３】情報処理装置２では、イニシャルプログラムが起動される。この場合の処理は、ステップＳ１００からステップＳ２４０までは、データ暗号化の際に説明した通りである。ＩＣカード３０においても同様である。勿論、使用者が異なれば、ＩＣカード３０も異なることから、ステップＳ１７０にて受信するＩＤも異なり、ステップＳ２１０にてＩＣカード３０へ送信される暗号化された第２の暗／復号化処理プログラムも異なる。

【００９４】例えば、使用者のＩＤがＩＤaであれば、暗号化された第２の暗／復号化処理プログラムＰr1が対応していることから、暗号化された第２の暗／復号化処理プログラムＰr1が、ＩＣカード３０へ送信され、その結果、ステップＳ２４０により起動されるプログラムは、第２の暗／復号化処理プログラムＰr1が実行される。尚、ここでは、第２の暗／復号化処理プログラムＰr1は第２の暗／復号化処理プログラムＰr2と同じ内容であるとして説明する。

【００９５】ステップＳ２４０にて第２の暗／復号化処理プログラムＰr1が起動されると、まず、図９に示すフローチャートのステップＳ１０１０にて、処理メニューの表示がなされる。ここで使用者が復号化処理を選択すると、ステップＳ１２００の処理が開始される。この復号化処理を図１１のフローチャートに示す。

【００９６】まず、復号化対象データ名入力の要求が表示される（Ｓ１２０２）。次にステップＳ１２０６にてタイムアウトと判定されるまでその入力待ち（Ｓ１２０

４）となる。入力がなされずにタイムアウトとなればステップＳ１２０６にて肯定判定されて、第２の暗／復号化処理を終了し、イニシャルプログラムに帰る。

【００９７】光磁気ディスクドライブ１４にセットされた光磁気ディスク内の一つのデータファイルを指定した場合（光磁気ディスク内のファイルすべてを指定しても良いし、特定のディレクトリ内のファイルをすべて指定しても良い。）、ステップＳ１２０４にて肯定判定されて、その復号化対象の暗号化データのヘッダー部より復号化対象者ＩＤ(1)，ＩＤ(2)，…および対応する暗号化された一時鍵Ｋ(1)，Ｋ(2)，…を読み出す（Ｓ１２０８）。

【００９８】次にこの復号化対象者ＩＤ(1)，ＩＤ(2)，…内に、使用者のＩＤが存在するか否かが判定される（Ｓ１２１０）。すなわち、ＩＣカードリーダー２６にセットされているＩＣカード３０に記載されている使用者のＩＤが、復号化対象者として指定されているか否かが判定される。存在しなければ、現在セットされているＩＣカード３０の正当な使用者は、復号化は許可されていないので、ステップＳ１２１０にて否定判定されて、復号化は不許可であることをＣＲＴディスプレイ１６に表示して（Ｓ１２２０）、第２の暗／復号化処理を終了して、イニシャルプログラムに戻る。尚、複数のファイルが復号化対象として指示された場合には、ＩＣカード３０に記載されている使用者のＩＤが復号化対象者としてヘッダー部に指定されているファイルが一つでも存在すれば、その含まれているファイルについてだけステップＳ１２３０以降の処理を行う。また、ヘッダー部にグループのＩＤが指定されている場合には、ＩＣカード３０の正当使用者がそのグループに含まれていれば、その正当使用者はヘッダー部に指定されているとする。

【００９９】ＩＣカード３０に記載された正当な使用者のＩＤが、復号化対象者ＩＤ(1)，ＩＤ(2)，…内に含まれている場合、例えば、ＩＤ(1)が該当すると、ステップＳ１２１０にて肯定判定されて、復号化対象ファイルのヘッダー部から読み出した暗号化された一時鍵Ｋ(1)を、ＩＣカード３０側へ送信し（Ｓ１２３０）、次に復号化された一時鍵の受信待ち（Ｓ１２４０）となる。

【０１００】ＩＣカード３０側にて、ステップＳ５９０，Ｓ５９５およびＳ６００を繰り返している状態で、暗号化された一時鍵Ｋ(1)を受信すると、ステップＳ５９５にて肯定判定されて、一時鍵復号化処理プログラムＰｒ15により、暗号化された一時鍵Ｋ(1)を、バックアップＲＡＭ３８に記憶している正当な使用者の暗／復号化鍵で復号化する（Ｓ６３０）。

【０１０１】次に復号化された一時鍵を情報処理装置２へ送信し（Ｓ６４０）、ステップＳ５００の処理に戻る。情報処理装置２側では、復号化された一時鍵を受信したので、ステップＳ１２４０にて肯定判定されて、復号化対象データのデータ部を復号化された一時鍵で復号化して記憶媒体に格納する（Ｓ１２５０）。

【０１０２】こうして復号化処理（Ｓ１２００）が終了すると、前述したステップＳ１５００にて、ＲＡＭ８上に暗号化されていないデータ、すなわち復号化されたデータが存在する場合には、そのデータをクリアする処理が行われる。こうして、第２の暗／復号化処理が終了し、イニシャルプログラムに戻る。イニシャルプログラムでは、図６に示すステップＳ２５０の処理が行われて、ＲＡＭ８上に存在している第２の暗／復号化処理プログラムをクリアし、ステップＳ１１０の処理に戻る。

【０１０３】このようにして、データの復号化が終了する。上述したごとく、本実施例の情報処理装置２にて起動する復号化処理用のプログラム（図９，図１１）は、復号化処理に用いられていない場合には、ハードディスク装置１８により暗号化された状態で記憶されている。したがって、第三者により、解析されることはなく、また解析できないので改竄もできない。

【０１０４】正当な使用者が復号化データを復号化する場合には、ハードディスク装置１８から、正当な使用者の暗／復号化鍵にて暗号化された前記プログラムを読み出し、そのプログラムを、正当な使用者の暗／復号化鍵により復号化し、その復号化されたプログラムを起動させることにより、暗号化データを一時鍵（第２復号化鍵に該当する。すなわち一時鍵は第２暗号化鍵でも有り、第２復号化鍵でもある。）にて復号化させて復号化データ、すなわち平文データとすることができる。

【０１０５】しかも、暗号化データの復号化が完了した後は、その起動されたプログラムを消去する。このため、復号化処理をした後も、平文状態の復号化用のプログラムが残っていることもなく、復号化用のプログラムの安全性が確保され、結果として、データの安全性も確保される。したがって、復号化処理毎に、復号化処理用のプログラムを記憶している記憶媒体を保管場所から取り出して情報処理装置２にセットしてロードする作業をしなくても良く、効率的に復号化作業ができる。

【０１０６】また、復号化されたデータも作業メモリ領域上に残っている場合には、それをクリアしているので、より安全性が高い。更に、暗号化データに含まれる暗号化された一時鍵（第２復号化鍵）を、正当な使用者の暗／復号化鍵にて復号化する。

【０１０７】このようにすることにより、暗号化データを復号化するための一時鍵（第２復号化鍵）が得られ、正当な使用者のみが適切に暗号化データを復号化して平文データを得ることができる。また、本実施例では、本体装置としての情報処理装置２と、この情報処理装置２とは別体に構成され情報処理装置２に対して信号的に任意に接続したり切断したりすることが可能な付属装置としてのＩＣカード３０とに別れて構成され、情報処理装置２が、プログラム暗号化記憶処理、プログラム読出処理、プログラム起動処理、およびプログラム消去処理の

各プログラムを備え、ＩＣカード３０が、正当な使用者の暗／復号化鍵を記憶するとともに、プログラム復号化処理および鍵復号化処理のプログラムを備える構成とされている。

【０１０８】このように構成されているため、ＩＣカード３０側には、正当な使用者の暗／復号化鍵、プログラム復号化処理および鍵復号化処理のプログラムが存在するため、その正当な使用者に対応する暗／復号化鍵、プログラム復号化処理のプログラムおよび鍵復号化処理のプログラムの安全性が確保され、データの安全性が一層確保される。

【０１０９】次に、ハードディスク装置１８に記憶されている、暗号化された第２の暗復号化処理プログラムの変更処理について説明する。使用者は、まず、情報処理装置２の電源オンさせた後、受け取った光磁気ディスクを光磁気ディスクドライブ１４にセットし、自己のＩＣカード３０をＩＣカードリーダー２６にセットする。

【０１１０】情報処理装置２では、イニシャルプログラムが起動される。この場合の処理は、ステップＳ１００からステップＳ２４０までは、データ暗号化あるいは復号化の際に説明した通りである。ＩＣカード３０においても同様である。勿論、使用者が異なれば、ＩＣカード３０も異なることから、ステップＳ１７０にて受信するＩＤも異なり、ステップＳ２１０にてＩＣカード３０へ送信される暗号化された第２の暗／復号化処理プログラムも異なる。

【０１１１】例えば、使用者のＩＤがＩＤcであれば、暗号化された第２の暗／復号化処理プログラムPr3が対応していることから、暗号化された第２の暗／復号化処理プログラムPr3が、ＩＣカード３０へ送信され、その結果、ステップＳ２４０により起動されるプログラムは、第２の暗／復号化処理プログラムPr3が実行される。　ステップＳ２４０にて第２の暗／復号化処理プログラムPr3が起動されると、まず、図９に示すフローチャートのステップＳ１０１０にて、処理メニューの表示がなされる。

【０１１２】ここで使用者がプログラム変更処理を選択すると、ステップＳ１３００の処理が開始される。プログラム変更処理を図１２のフローチャートに示す。まず、第２の暗／復号化処理プログラムの編集処理がなされる（Ｓ１３０２）。例えば、１６進数にて表現されている第２の暗／復号化処理プログラムを逆アセンブルして、アセンブリ言語にて表現し、キーボード１２による編集可能とする。編集が終了すれば、編集後の内容がアセンブルされ、実行可能なプログラムに変換される。

【０１１３】尚、この編集処理では、単に既に変更されている他のプログラムと置き換える処理も含まれる。したがって、他の装置で作成したプログラムを新たに、第２の暗／復号化処理プログラムとして取り込むことができる。また、この編集処理では、単にプログラム中に設定されている数値や文字列等のデータの変更も含まれる。

【０１１４】次に、編集後の第２の暗／復号化処理プログラムをＩＣカード３０側へ送信し（Ｓ１３０４）、暗号化された第２の暗／復号化処理プログラムの受信待ち（Ｓ１３０６）となる。ＩＣカード３０側にて、ステップＳ５９０，Ｓ５９５およびＳ６００を繰り返している状態で、暗号化していない第２の暗／復号化処理プログラムを受信すると、ステップＳ６００にて肯定判定されて、プログラム暗号化処理プログラムＰｒ12により、ＩＣカード３０の正当な使用者の暗／復号化鍵により第２の暗／復号化処理プログラムを暗号化する（Ｓ６５０）。

【０１１５】次に、この暗号化された第２の暗／復号化処理プログラムを情報処理装置２へ送信し（Ｓ６６０）、ステップＳ５００の処理に戻る。情報処理装置２側では、暗号化された第２の暗／復号化処理プログラムを受信したので、ステップＳ１３０６にて肯定判定され、次に暗号化された第２の暗／復号化処理プログラムをハードディスク装置１８に収納し、そのディスクアドレスを、使用者ＩＤ－プログラムアドレステーブルの内、ＩＤcと対応させたプログラムアドレスＰｒ3に記入する（Ｓ１３０８）。

【０１１６】こうして、プログラム変更処理を終了する。以後、ステップＳ１５００の処理を行って、イニシャルプログラムに帰る。イニシャルプログラムでは、ステップＳ２５０の処理が行われて、ＲＡＭ８上に存在している第２の暗／復号化処理プログラムをクリアし、ステップＳ１１０の処理に戻る。

【０１１７】上述したごとく、本実施例の情報処理装置２にて起動するプログラム変更処理（図９，図１２）は、正当な使用者により、その使用者専用の暗号化された第２の暗／復号化処理プログラムの内容を変更できるので、その使用者毎に異なるアルゴリズムや異なる設定値（プログラム中のデータを変更した場合）にて暗／復号化することが可能となる。

【０１１８】したがって、使用者毎にプログラムを変更しておけば、一人の暗／復号化アルゴリズムが第三者に解析された場合にも、同時に全員のプログラムまで解析されることはない。また、解析された場合には、プログラム変更処理により、正当な使用者がプログラムを変更することにより、以後の情報については安全性が確保できる。

【０１１９】また本実施例において、入力操作が行われない場合は、タイムアウト処理（Ｓ１１０６，Ｓ１２０６）により第２の暗／復号化処理プログラムを終了し、ステップＳ２５０のの処理が行われて、ＲＡＭ８上に存在している第２の暗／復号化処理プログラムをクリアしているので、使用者が処理の途中で情報処理装置２を離れても、第三者による解析や改竄を防止できる。ステッ

プＳ１３０２にても編集の途中で操作が行われなくなれば、第２の暗／復号化処理プログラムを終了しても良い。

【０１２０】また、情報処理装置２側では、データ量の大きい暗号化対象のデータの暗号化あるいは復号化処理を行い、ＩＣカード３０側では、データ量の小さいプログラムや一時鍵の暗号化あるいは復号化処理を行うので、全体の処理としては高速に行うことができる。また、ＩＣカード３０としては小さくて安価な構成とすることができる。

【０１２１】また、図１３に示したごとく、復号化を許可する者の数に対応して暗号化されるのは一時鍵のみであり、実際の暗号化データは一つのみ存在することから、保管、運搬あるいは通信するデータ量は、復号化を許可する者の数が多くても、膨大なデー多量とはならず、メモリや記憶媒体あるいは通信時間が節約できる。

【０１２２】本実施例において、ハードディスク装置１８がプログラム暗号化記憶手段に該当し、ステップＳ２１０がプログラム読出手段としての処理に該当し、ステップＳ５７０がプログラム復号化手段としての処理に該当し、ステップＳ２４０がプログラム起動手段としての処理に該当し、ステップＳ２５０がプログラム消去手段としての処理に該当し、ステップＳ６１０が鍵暗号化手段としての処理に該当し、ステップＳ１１６０が鍵付加手段としての処理に該当し、ステップＳ６３０が鍵復号化手段としての処理に該当する。

【０１２３】［その他］上述した実施例は、データを暗号化したり、あるいは暗号化したデータを復号化して平文データに戻す情報秘匿処理システムであったが、更に、情報処理装置２が網制御装置およびモデムを備えることにより、正当な使用者が前記実施例のごとくデータを暗号化して通信回線を介して相手方に送信し、また相手方が通信回線を介して送信して来た暗号化データを、前記実施例のごとく正当な使用者（復号化対象者）が復号化して平文データとして得る情報秘匿通信システムとして構成しても良い。

【０１２４】更に、この情報秘匿通信システムに、原稿の画像読取装置および画像の記録装置を備えることにより、ファクシミリ装置として構成し、その原稿の画像データを、前記実施例のごとく、暗号化あるいは復号化の対象としても良い。前記実施例では、正当使用者や復号化対象者をＩＤで指定していたが、ＩＤでなくても対象者名でも良いし、ＩＤと対象者名との両方でも良い。

【０１２５】前記実施例では、ＩＣカード３０に記憶されている正当使用者の暗／復号化鍵は、暗号化にも復号化にも用いられたが、暗号化時は公開鍵を用い、復号化時には秘密鍵を用いても良い。したがって、正当な使用者がデータの復号化を許可する相手方暗号化鍵Ｋ1，Ｋ2，…，Knは公開鍵であっても良い。

【０１２６】またＩＣカード３０のバックアップＲＡＭ３８には、復号化を許可する相手方のＩＤ1，ＩＤ2，…とそれに対応した暗号化鍵Ｋ1，Ｋ2，…とが記憶されていたが、直接、このようなＩＤと暗号化鍵Ｋとを記憶するのではなく、次のようにしても良い。

【０１２７】すなわち、バックアップＲＡＭ３８に秘密のアルゴリズムを内蔵し、復号化を許可する相手方のＩＤを入力すると、そのアルゴリズムにしたがって演算処理にて対応する暗号化鍵Ｋを生成する構成としても良い。この構成にすると複数の暗号化鍵を記憶しなくても、一つのアルゴリズムのみで、多数のＩＤから暗号化鍵を得ることができるので、復号化を許可する者が多い場合には、メモリの節約となる。

【０１２８】このＩＤから演算処理で鍵を生成する構成を、ＩＣカード３０の正当な使用者の暗／復号化鍵に対しても適用して、正当な使用者のＩＤから暗／復号化鍵を生成するようにしても良い。また、ＩＣカード３０は、バックアップＲＡＭ３８にプログラムや各鍵等を保管しているので、外装に連動して外装開放時にオフとなるスイッチをバックアップ電源とバックアップＲＡＭ３８との間に用いれば、外装を開けるとプログラムや鍵等が消去されることから、安全上、より好ましい。また、バックアップＲＡＭ３８の代りに、ＥＥＰＲＯＭにプログラムや鍵等を記憶しても良い。この場合は、外装と連動して外装開放時にオンとなるスイッチを電源とＥＥＰＲＯＭとの間に設ければ、外装を開けると電流が流れてプログラムや鍵等が消去される。

【０１２９】前記実施例において、イニシャルプログラムはハードディスク装置１８でなく、ＲＯＭ６に格納されていても良い。

【図面の簡単な説明】

【図１】　本発明一実施例を構成する情報処理装置のブロック図である。

【図２】　本発明一実施例を構成するＩＣカードのブロック図である。

【図３】　情報処理装置におけるプログラムおよびデータの記憶配置説明図である。

【図４】　ＩＣカードにおけるプログラムおよびデータの記憶配置説明図である。

【図５】　情報処理装置におけるイニシャルプログラムのフローチャートである。

【図６】　情報処理装置におけるイニシャルプログラムのフローチャートである。

【図７】　ＩＣカード側処理のフローチャートである。

【図８】　ＩＣカード側処理のフローチャートである。

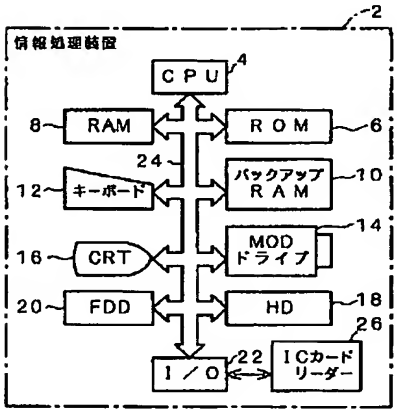
【図９】　第２の暗／復号化処理のフローチャートである。

【図１０】　第２の暗／復号化処理の内の暗号化処理のフローチャートである。

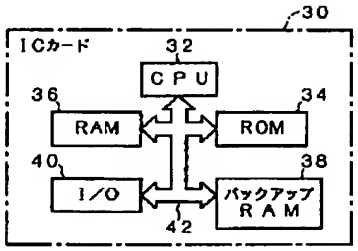
【図１１】　第２の暗／復号化処理の内の復号化処理のフローチャートである。

【図１２】　第２の暗／復号化処理の内のプログラム変更処理のフローチャートである。
【図１３】　暗号化データの構成説明図である。
【符号の説明】
２…情報処理装置　　４…ＣＰＵ　　６…ＲＯＭ　　８…ＲＡＭ
１０…バックアップＲＡＭ　　１２…キーボード
１４…光磁気ディスクドライブ　　１６…ＣＲＴディスプレイ
１８…ハードディスク装置　　２０…フロッピーディスクドライブ
２２…Ｉ／Ｏ　　２４…バス　　２６…ＩＣカードリーダー
３０…ＩＣカード　　３２…ＣＰＵ　　３４…ＲＯＭ　　３６…ＲＡＭ
３８…バックアップＲＡＭ　　４０…Ｉ／Ｏ　　４２…バス

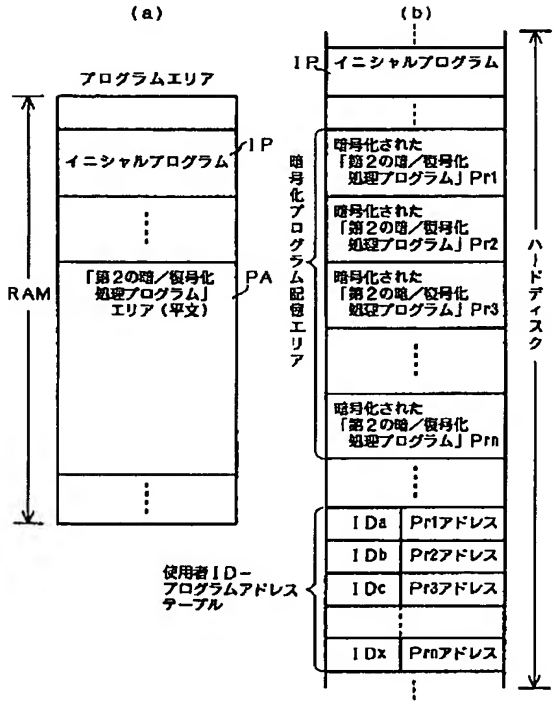
【図１】



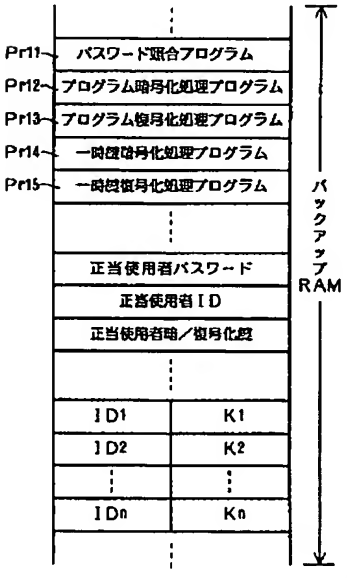
【図２】



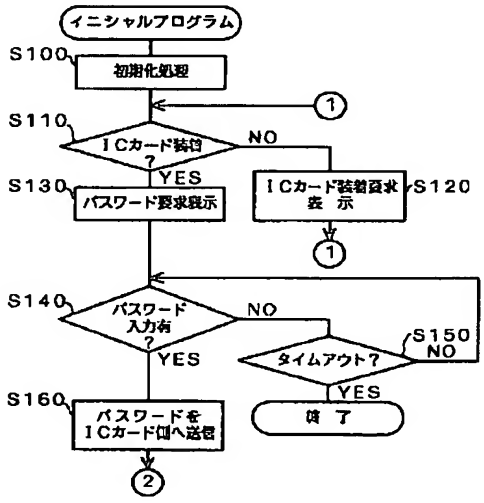
【図３】



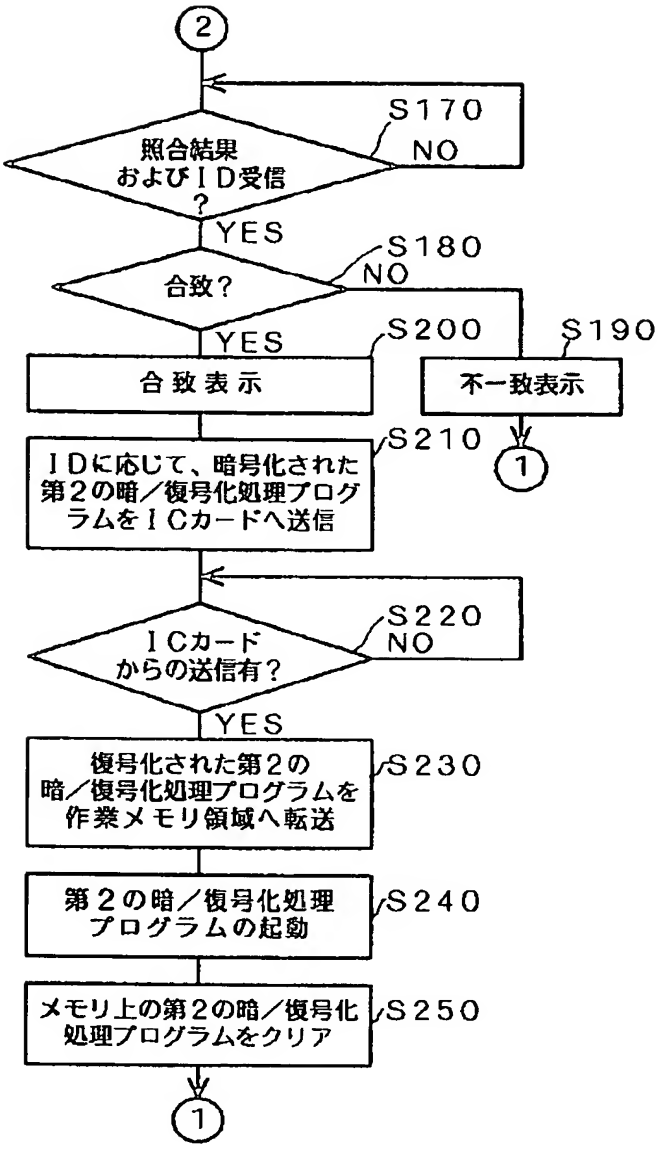
【図４】



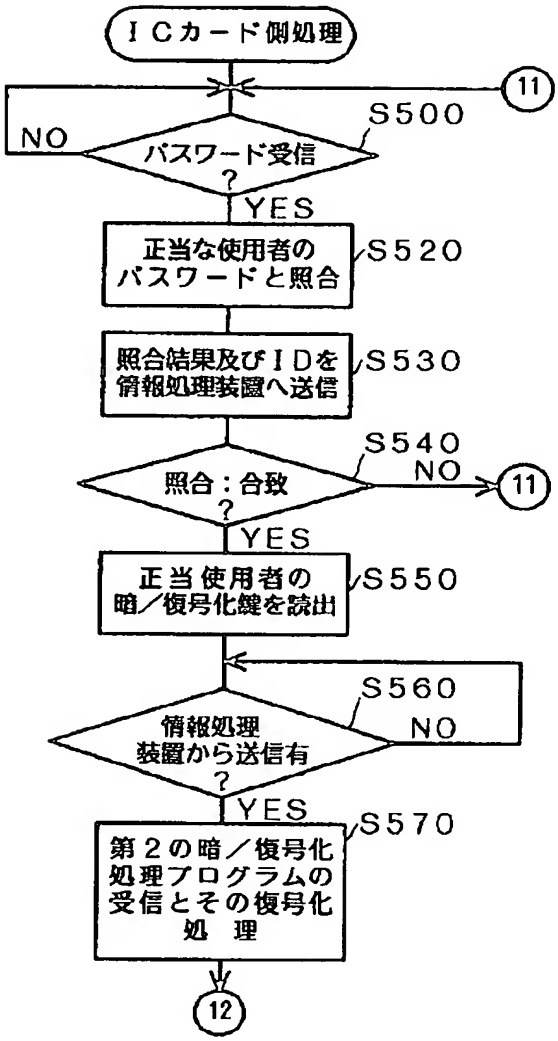
【図５】



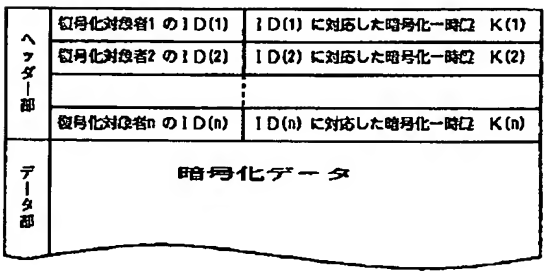
【図６】


2
照合結果およびＩＤ受信？
S170
NO
YES
合致？
S180
NO
YES
S200
合致表示
S190
不一致表示
1
ＩＤに応じて、暗号化された第２の暗／復号化処理プログラムをＩＣカードへ送信
S210
ＩＣカードからの送信有？
S220
NO
YES
復号化された第２の暗／復号化処理プログラムを作業メモリ領域へ転送
S230
第２の暗／復号化処理プログラムの起動
S240
メモリ上の第２の暗／復号化処理プログラムをクリア
S250
1

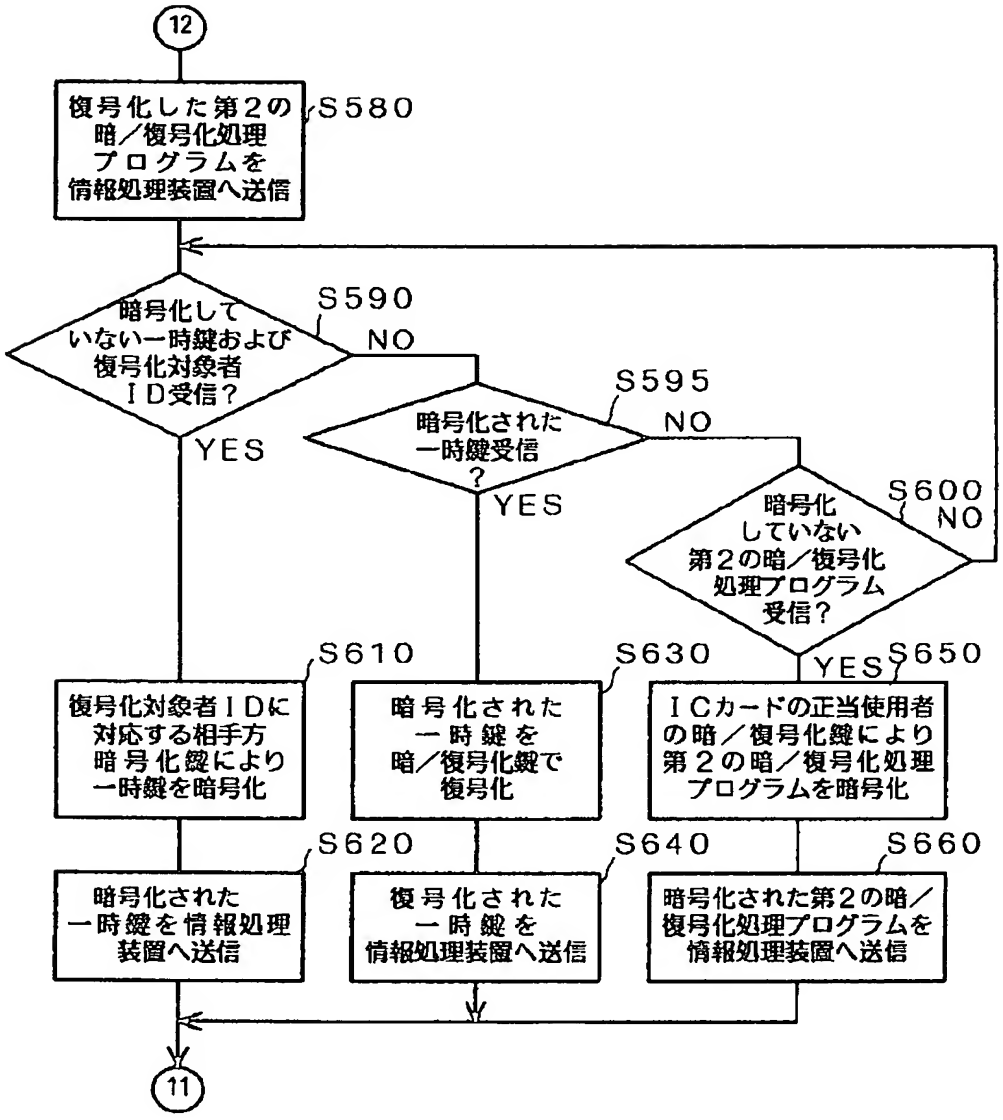
【図７】


ＩＣカード側処理
11
NO
パスワード受信？
S500
YES
正当な使用者のパスワードと照合
S520
照合結果及びＩＤを情報処理装置へ送信
S530
照合：合致？
S540
NO
11
YES
正当使用者の暗／復号化鍵を読出
S550
情報処理装置から送信有？
S560
NO
YES
第２の暗／復号化処理プログラムの受信とその復号化処理
S570
12

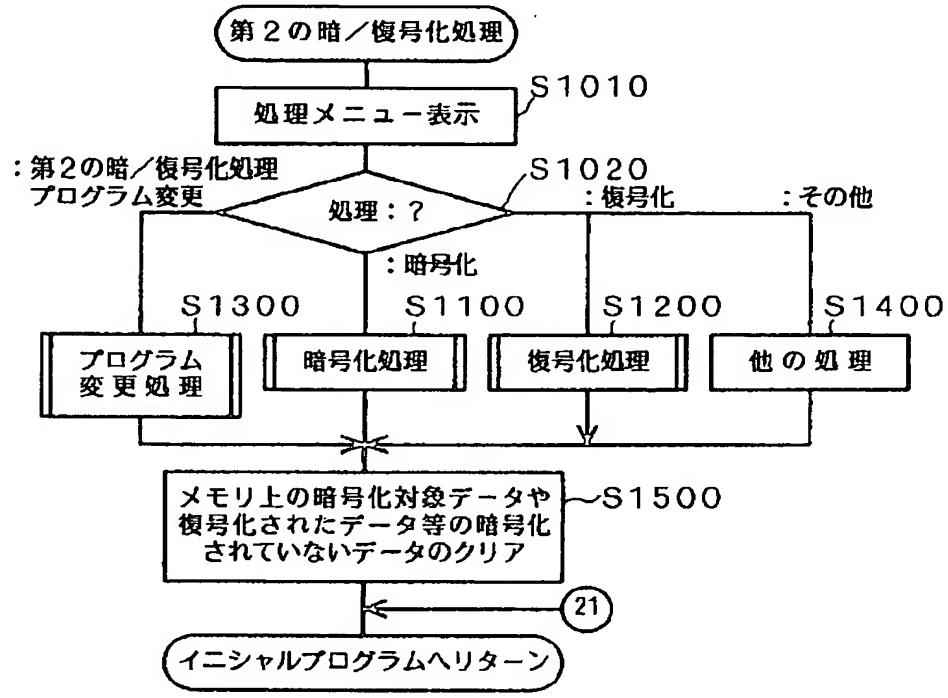
【図１３】


ヘッダー部
復号化対象者1 のＩＤ(1)
ＩＤ(1) に対応した暗号化一時鍵 K(1)
復号化対象者2 のＩＤ(2)
ＩＤ(2) に対応した暗号化一時鍵 K(2)
復号化対象者n のＩＤ(n)
ＩＤ(n) に対応した暗号化一時鍵 K(n)
データ部
暗号化データ

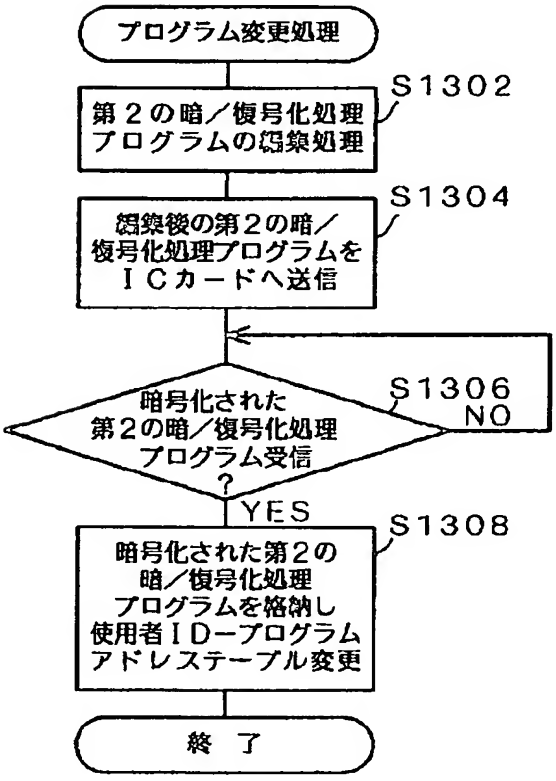
【図8】


12
複号化した第2の暗／複号化処理プログラムを情報処理装置へ送信
S580
暗号化していない一時鍵および複号化対象者ID受信？
S590
NO
YES
暗号化された一時鍵受信？
S595
NO
YES
暗号化していない第2の暗／複号化処理プログラム受信？
S600
NO
YES
S610
複号化対象者IDに対応する相手方暗号化鍵により一時鍵を暗号化
S630
暗号化された一時鍵を暗／複号化鍵で複号化
S650
ICカードの正当使用者の暗／複号化鍵により第2の暗／複号化処理プログラムを暗号化
S620
暗号化された一時鍵を情報処理装置へ送信
S640
複号化された一時鍵を情報処理装置へ送信
S660
暗号化された第2の暗／複号化処理プログラムを情報処理装置へ送信
11

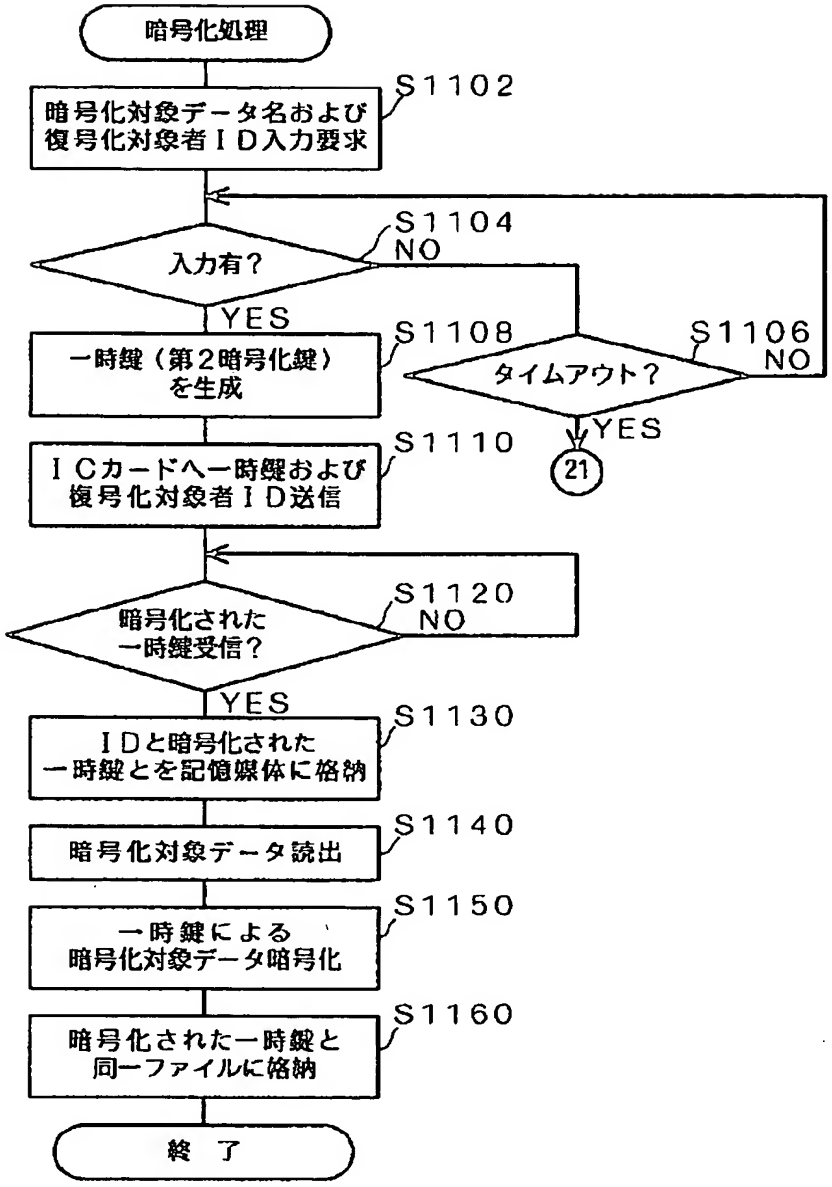
【図９】


第２の暗／復号化処理
処理メニュー表示
S1010
：第２の暗／復号化処理プログラム変更
処理：？
S1020
：復号化
：その他
：暗号化
S1300
S1100
S1200
S1400
プログラム変更処理
暗号化処理
復号化処理
他の処理
メモリ上の暗号化対象データや復号化されたデータ等の暗号化されていないデータのクリア
S1500
21
イニシャルプログラムへリターン

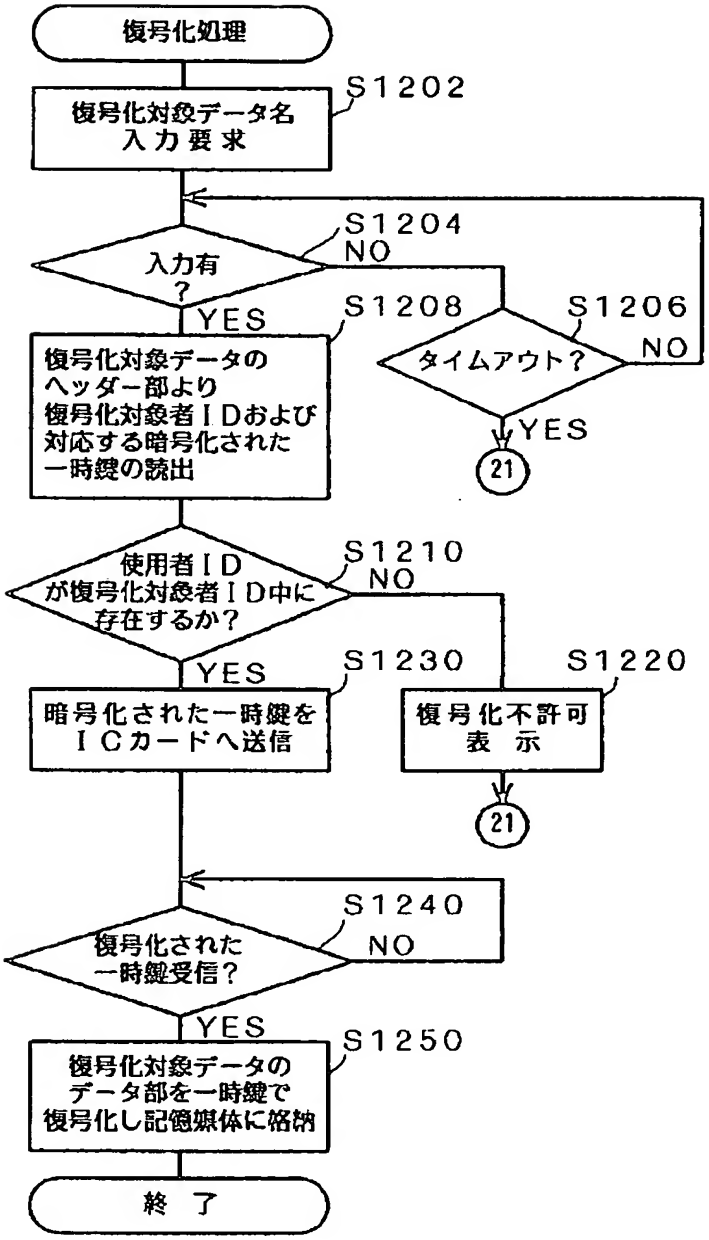
【図１２】


プログラム変更処理
第２の暗／復号化処理プログラムの構築処理
S1302
構築後の第２の暗／復号化処理プログラムをＩＣカードへ送信
S1304
暗号化された第２の暗／復号化処理プログラム受信？
S1306
NO
YES
暗号化された第２の暗／復号化処理プログラムを格納し使用者ＩＤ－プログラムアドレステーブル変更
S1308
終　了

【図１０】


暗号化処理
暗号化対象データ名および復号化対象者ＩＤ入力要求
S1102
入力有？
S1104
NO
YES
一時鍵（第２暗号化鍵）を生成
S1108
タイムアウト？
S1106
NO
YES
21
ＩＣカードへ一時鍵および復号化対象者ＩＤ送信
S1110
暗号化された一時鍵受信？
S1120
NO
YES
ＩＤと暗号化された一時鍵とを記憶媒体に格納
S1130
暗号化対象データ読出
S1140
一時鍵による暗号化対象データ暗号化
S1150
暗号化された一時鍵と同一ファイルに格納
S1160
終　了

【図11】


復号化処理
S1202
復号化対象データ名
入力要求
S1204
NO
入力有
？
YES
S1208
復号化対象データの
ヘッダー部より
復号化対象者ＩＤおよび
対応する暗号化された
一時鍵の読出
S1206
タイムアウト？
NO
YES
21
使用者ＩＤ
が復号化対象者ＩＤ中に
存在するか？
S1210
NO
YES
S1230
暗号化された一時鍵を
ＩＣカードへ送信
S1220
復号化不許可
表　示
21
S1240
NO
復号化された
一時鍵受信？
YES
S1250
復号化対象データの
データ部を一時鍵で
復号化し記憶媒体に格納
終　了

[JP,09-006232,A]

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

[Detailed Description of the Invention]

[0001]

[Industrial Application] This invention relates to the encryption system which enciphers data by encryption processing based on a program, the decryption system which decrypts encryption data by decryption processing based on a program, the information secrecy processing system which has these functions further, and information secrecy communication system.

[0002]

[Description of the Prior Art] The processing which enciphers information to keep it secret, using an encryption key as technique for keeping secret conventionally the contents of information (it also being called "data".) is known. Since it cannot return to the condition that human being can decode unless it uses the same encryption key or a specific decryption key once information is enciphered, for others who have neither such an encryption key nor the decryption key, the contents of the information can be made secret.

[0003] However, if an encryption key and a decryption key (it expresses as "dark / a decryption key" hereafter.) are revealed, since information will be instantly decoded by others, the file security system which raises safety is proposed by enciphering and keeping it with another encryption key also to this dark / decryption key (JP,6-102822,A).

[0004]

[Problem(s) to be Solved by the Invention] However, the following problems existed also in such a system. That is, as for the decryption processing for informational encryption processing or information decode, generally, it is common to be made by an encryption program or the decryption program (for it to express as an "encryption / decryption program" hereafter) with the information processor which used the computer system.

[0005] In order for information to be enciphered by this encryption / decryption program and to raise safety further, when even its dark / decryption key enciphers, it is thought apparently that that information itself is very safe. However, the encryption / decryption program itself which performs this encryption and decryption has that it is [much] more nearly defenseless than the information itself. When the algorithm of this encryption / decryption program is analyzed by the third person, there is a possibility that it may be used for decode of the enciphered information.

[0006] Moreover, there is also a possibility that a third person may decode all the enciphered information after that, by a third person's altering the encryption / decryption program itself so that a just user may not understand, and adding the function enciphered with the encryption key which the third person knows. Furthermore, there was also a possibility of adding the function which copies the information on the plaintext condition (the condition of not being

enciphered is said.) before enciphering also to the field which a third person manages in encryption / decryption program.

[0007] Of course, although keeping encryption / decryption program severely is also considered when not using encryption / decryption program, the processing which takes out a floppy etc. from a storage area, sets in an information processor for every use, and loads encryption / decryption program must be carried out, and encryption / decryption processing cannot carry out efficiently.

[0008] This invention aims at offering the encryption system which can perform encryption and a decryption efficiently, a decryption system, an information secrecy processing system, and information secrecy communication system, without being altered by the third person.

[0009]

[Means for Solving the Problem] In the encryption system as which invention according to claim 1 enciphers data by encryption processing based on a program A program encryption storage means to memorize said program in the condition of having enciphered with the 1st encryption key corresponding to a user, The program read-out means which reads said program enciphered with the 1st encryption key corresponding to a user from the inside of said program encryption storage means, By starting the program decrypted by program decryption means to decrypt said program read by said program read-out means with the decryption key corresponding to a user, and said program decryption means The program starting means which is made to encipher the data for encryption with the 2nd encryption key, and is used as encryption data, When the data encryption for encryption is completed with said program starting means, it is the encryption system characterized by having a program elimination means to eliminate said program which was decoded and became a candidate for starting.

[0010] Invention according to claim 2 is the encryption system according to claim 1 further equipped with a key encryption means to encipher said 2nd encryption key with the 3rd encryption key, and a key addition means to add said 2nd encryption key enciphered with said key encryption means to said encryption data.

[0011] Invention according to claim 3 is an encryption system according to claim 2 with which said key addition means is realized as a function of said program. Invention according to claim 4 is an encryption system according to claim 1 to 3 with which said program asks for the 2nd encryption key by the operation.

[0012] Invention according to claim 5 consists of attachment [the main frame and this main frame] which it is constituted by another object, and it connects with arbitration in signal, or can be cut to said main frame. While it has said program encryption storage means, said program read-out means, said program starting means, and said program elimination means and said attachment memorizes the decryption key corresponding to said user, said main frame It is an encryption system [equipped with said program decryption means] according to claim 1.

[0013] Invention according to claim 6 consists of attachment [the main frame and this main frame] which it is constituted by another object, and it connects with arbitration in signal, or can be cut to said main frame. Said main frame Said program encryption storage means, said program read-out means, It is the encryption system according to claim 3 with which it has said program decryption means, said program starting means, and said program elimination means, and it is equipped with said key encryption means while said attachment memorizes said 3rd encryption key.

[0014] Invention according to claim 7 consists of attachment [the main frame and this main frame] which it is constituted by another object, and it connects with arbitration in signal, or can be cut to said main frame. Said main frame Said program encryption storage means, said program read-out means, It is the encryption system according to claim 3 which is equipped with said program starting means and said program elimination means, and is equipped with said program decryption means and said key encryption means while said attachment memorizes the decryption key corresponding to said user, and said 3rd encryption key.

[0015] Invention according to claim 8 is an encryption system according to claim 6 or 7 with which said attachment remembers said 3rd encryption key to be Control Code of those who permit a decryption as a corresponding list. Invention according to claim 9 is an encryption system according to claim 5 to 7 which generates said decryption key or said 3rd encryption key by the operation using Control Code, when said attachment does not carry out immediate memory of said decryption key or said 3rd encryption key but said decryption key or said 3rd encryption key is needed.

[0016] Invention according to claim 10 is an encryption system according to claim 1 to 9 with which said program has the function to stop self processing and to perform processing of said program elimination means when the next alter operation is not performed by the user within predetermined time.

[0017] In the decryption system to which invention according to claim 11 decrypts encryption data by decryption processing based on a program A program encryption storage means to memorize said program in the condition of having enciphered with the 1st encryption key corresponding to a user, The program read-out means which reads said program enciphered with the 1st encryption key corresponding to a user from the inside of said program encryption storage means, By starting said program decrypted by program decryption means to decrypt said program read by said program read-out means with the decryption key corresponding to a user, and said program decryption means The program starting means which is made to decrypt encryption data with the 2nd decryption key, and is used as decryption data, When a decryption of encryption data is completed with said program starting means, it is the decryption system characterized by having a program elimination means to eliminate said program which was decrypted and became a candidate for starting.

[0018] Invention according to claim 12 is the decryption system [equipped with a key decryption means to decrypt the enciphered 2nd decryption key which is contained in said encryption data with the decryption key corresponding to a user further] according to claim 11.

[0019] Invention according to claim 13 consists of attachment [the main frame and this main frame] which it is constituted by another object, and it connects with arbitration in signal, or can be cut to said main frame. While it has said program encryption storage means, said program read-out means, said program starting means, and said program elimination means and said attachment memorizes the decryption key corresponding to said user, said main frame It is a decryption system [equipped with said program decryption means] according to claim 11.

[0020] Invention according to claim 14 consists of attachment [the main frame and this main frame] which it is constituted by another object, and it connects with arbitration in signal, or can be cut to said main frame. Said main frame Said program encryption storage means, said program read-out means, It is the decryption system according to claim 12 which is equipped with said program decryption means, said program starting means, and said program elimination means, and is equipped with said key decryption means while said attachment memorizes the decryption key corresponding to said user.

[0021] Invention according to claim 15 consists of attachment [the main frame and this main frame] which it is constituted by another object, and it connects with arbitration in signal, or can be cut to said main frame. While it has said program encryption storage means, said program read-out means, said program starting means, and said program elimination means and said attachment memorizes the decryption key corresponding to said user, said main frame It is a decryption system [equipped with said program decryption means and said key decryption means] according to claim 12.

[0022] Invention according to claim 16 is a decryption system according to claim 13 to 15 which generates said decryption key by the operation using Control Code, when said attachment does not carry out immediate memory of said decryption key but said decryption key is needed.

[0023] Invention according to claim 17 is a decryption system according to claim 11 to 16 by which said program has the function to stop self processing and to perform processing of said program elimination means when the next alter operation is not performed by the user within predetermined time.

[0024] Invention according to claim 18 is an information secrecy processing system with which it comes to put any of claims 1-10, the encryption system of a publication, and a decryption system according to claim 11 to 17 together. Invention according to claim 19 is any of claims 1-10 equipped with a transmitting means to transmit said encryption data to the other party through a communication line, or the encryption system of a publication.

[0025] Invention according to claim 20 is the decryption system of any of claims 11-17 equipped with a receiving means to receive said encryption data through a communication line, or a publication. Invention according to claim 21 is information secrecy communication system with which it comes to put an encryption system and a decryption system according to claim 20 according to claim 19 together.

[0026]

[Function and Effect(s) of the Invention] The encryption system of claim 1 is equipped with a program encryption storage means, a program read-out means, a program decryption means, a program starting means, and a program elimination means, and a program encryption storage means memorizes, where the program for encryption processing is enciphered with the 1st encryption key corresponding to a user. A program read-out means reads said program enciphered with the 1st encryption key corresponding to a user from the inside of said program encryption storage means. A program decryption means decrypts said program read by said program read-out means with the decryption key corresponding to a user. By starting the program decrypted by said program decryption means, a program starting means makes the data for encryption encipher with the 2nd encryption key, and let it be encryption data. A program elimination means will eliminate said program which was decoded and became a candidate for starting, if the data encryption for encryption is completed with said program starting means.

[0027] Thus, the program for encryption processing started with the encryption system of this invention is memorized in the condition of having been enciphered by the program encryption storage means, when not used for encryption processing. Therefore, since it cannot analyze and analyze by the third person while it had been enciphered, an alteration is also impossible. Moreover, when a user possesses, a decryption key cannot decrypt the program for encryption processing, even if a program decryption means becomes clear for a third person.

[0028] When a just user enciphers data, a program read-out means reads said program enciphered with the 1st encryption key corresponding to a user from the inside of a program encryption storage means, a program decryption means decrypts the program with the

decryption key corresponding to a user, and a program starting means starts the decrypted program. It is enciphered with the 2nd encryption key by this started function of said program, and the data for encryption turn into encryption data by it.

[0029] And after a data encryption is completed, a program elimination means eliminates the program of the started plaintext condition. For this reason, even after carrying out encryption processing, the program for encryption of a plaintext condition does not remain, the safety of the program for encryption is secured, and the safety of the enciphered data is also secured as a result. Therefore, it is not necessary to take out the storage which has memorized the program for encryption processing from a storage area for every encryption processing, and to do the activity set and loaded to a computer, and an encryption activity can be performed efficiently.

[0030] A key encryption means and a key addition means may be further added to the above-mentioned configuration. This key encryption means enciphers said 2nd encryption key with the 3rd encryption key. And a key addition means adds said 2nd encryption key enciphered with said key encryption means to said encryption data.

[0031] Thus, since the 2nd encryption key for enciphering data is further enciphered with the 3rd encryption key, insurance is securable even if it adds the 2nd encryption key to encryption data with the key addition means. Moreover, since the 2nd encryption key is added to encryption data, encryption data can be decrypted, if even the 3rd encryption key is kept at a carrying place or the communications-partner point even if it transmits carrying with the storage ****, or its encryption data to the other party by communication link. That is, encryption data can be decrypted with the 2nd encryption key which decrypted the enciphered 2nd encryption key which is added to encryption data with the 3rd encryption key, and then was decrypted. In addition, the key addition means may be realized as a function of the program for said encryption.

[0032] Furthermore, the 2nd encryption key may be called for by the operation by the program for said encryption in this case. Thus, the encryption key required in an operation is a temporary key, and since it is not used continuously, the safety of data is secured more. Moreover, since it is calculating by the program for the above-mentioned encryption, since only what was enciphered exists, this temporary key cannot alter the program which generates that 2nd encryption key except the time of encryption processing, either, so that the key which the third person knows may be generated.

[0033] Moreover, this encryption system separates to the attachment [the main frame and this main frame] which it is constituted by another object, and it connects with arbitration in signal, or can be cut to said main frame, and may be constituted. For example, the configuration which uses the main frame as a computer apparatus and uses attachment as an IC card is mentioned.

[0034] In this case, the main frame is good also as a configuration which is equipped with said program encryption storage means, said program read-out means, said program starting means, and said program elimination means, and is equipped with said program decryption means while memorizing the decryption key corresponding to said user in attachment.

[0035] Thus, if constituted, when not carrying out encryption processing, attachment can be separated from the main frame and it can contain to a safe storage area. Since the decryption key and program decryption means corresponding to a user exist, both the safeties of the program of the decryption key and a program decryption means are secured, and the safety of data is further secured to an attachment side.

[0036] Moreover, similarly, when separately constituted by the main frame and attachment, it is good as a configuration which the main frame equips with said program encryption storage

means, said program read-out means, said program decryption means, said program starting means, and said program elimination means, and is equipped with said key encryption means while attachment memorizes said 3rd encryption key.

[0037] Thus, if constituted, since the 3rd encryption key and a key encryption means exist, both the safeties of the program of the 3rd encryption key and a key encryption means will be secured, and the safety of data will be further secured to an attachment side. Moreover, when separately constituted by the main frame and attachment, while the configuration which considered above-mentioned both, i.e., the main frame, is equipped with said program encryption storage means, said program read-out means, said program starting means, and said program elimination means and attachment memorizes the decryption key corresponding to said user, and said 3rd encryption key, it is good also as a configuration which it has in said program decryption means and said key encryption means.

[0038] Thus, if constituted, since the decryption key corresponding to a user, the 3rd encryption key, a program decryption means, and a key encryption means exist, all the safeties of the program of the decryption key corresponding to the user, the 3rd encryption key, and a program decryption means and the program of a key encryption means will be secured, and the safety of data will be further secured to an attachment side.

[0039] Moreover, said attachment may memorize as a list with which the decryption was corresponded in the 3rd encryption key with a person's Control Code to permit. Thus, if are constituted and those who permit a decryption by Control Code, for example, ID, will be specified, the key encryption means of attachment can encipher the 2nd encryption key with the 3rd encryption key corresponding to the ID.

[0040] Moreover, when said attachment did not carry out immediate memory of a decryption key or the 3rd encryption key but the decryption key or the 3rd encryption key was needed, it is good also as what generates a decryption key or the 3rd encryption key by the operation using Control Code. When many 3rd encryption keys must memorize especially, since it is good only at operation expression, it becomes saving of memory.

[0041] Moreover, said program is good also as what has the function to stop self processing and to perform processing of said program elimination means, when the next alter operation is not performed by the user within predetermined time. If it does in this way, even if a just user will once separate from a system unit, since the program of a plaintext condition itself disappears after a while, it is analyzed by the third person or is not altered.

[0042] The decryption system of claim 11 A program encryption storage means, a program read-out means, It has a program decryption means, a program starting means, and a program elimination means. A program encryption storage means Said program is memorized in the condition of having enciphered with the 1st encryption key corresponding to a user. A program read-out means Said program enciphered with the 1st encryption key corresponding to a user is read from the inside of said program encryption storage means. A program decryption means Said program read by said program read-out means is decrypted with the decryption key corresponding to a user. A program starting means By starting said program decrypted by said program decryption means, encryption data are made to decrypt with the 2nd decryption key, and it considers as decryption data. A program elimination means If a decryption of encryption data is completed with said program starting means, said program which was decrypted and became a candidate for starting will be eliminated.

[0043] Thus, the program for decryption processing started by the decryption system of this invention is memorized in the condition of having been enciphered by the program encryption storage means, when not used for decryption processing. Therefore, since it cannot analyze and analyze by the third person while it had been enciphered, an alteration is also impossible.

Moreover, when a user possesses, a decryption key cannot decrypt the program for decryption processing, even if a program decryption means becomes clear for a third person.

[0044] When a just user decrypts encryption data, a program read-out means reads said program enciphered with the 1st encryption key corresponding to a user from the inside of a program encryption storage means, a program decryption means decrypts the program by the decryption key corresponding to a user, and a program starting means starts the decrypted program. By this started function of said program, encryption data can be made to be able to decrypt with the 2nd decryption key, and it can carry out to decryption data, i.e., plaintext data.

[0045] And after a decryption of encryption data is completed, a program elimination means eliminates the program of the started plaintext condition. For this reason, without the program for a decryption of a plaintext condition remaining, even after carrying out decryption processing, the safety of the program for a decryption is secured and the safety of data is also secured as a result. Therefore, it is not necessary to take out the storage which has memorized the program for decryption processing from a storage area for every decryption processing, and to do the activity set and loaded to a computer, and a decryption can be done efficiently.

[0046] Key decryption ****** may be further added to the above-mentioned configuration. This key decryption means decrypts the enciphered 2nd decryption key which is contained in encryption data with the decryption key corresponding to a user. By doing in this way, the 2nd decryption key for decrypting encryption data is obtained, and only a just user can decrypt encryption data appropriately and can get plaintext data.

[0047] Moreover, this decryption system separates to the attachment [the main frame and this main frame] which it is constituted by another object, and it connects with arbitration in signal, or can be cut to said main frame, and may be constituted. For example, the configuration which uses the main frame as a computer apparatus and uses attachment as an IC card is mentioned.

[0048] In this case, the main frame is good also as a configuration which is equipped with said program encryption storage means, said program read-out means, said program starting means, and said program elimination means, and is equipped with said program decryption means while memorizing the decryption key corresponding to said user in attachment.

[0049] Thus, if constituted, when not carrying out decryption processing, attachment can be separated from the main frame and it can contain to a safe storage area. Since the decryption key and program decryption means corresponding to a user exist, both the safeties of the program of the decryption key and a program decryption means are secured, and the safety of data is further secured to an attachment side.

[0050] Moreover, similarly, when separately constituted by the main frame and attachment, the main frame is good as a configuration which is equipped with said program encryption storage means, said program read-out means, said program decryption means, said program starting means, and said program elimination means, and is equipped with said key decryption means while memorizing the decryption key corresponding to a user in attachment.

[0051] Thus, if constituted, since the decryption key and key decryption means corresponding to a user exist, both the safeties of the program of the decryption key and a key decryption means will be secured, and the safety of data will be further secured to an attachment side. Moreover, when separately constituted by the main frame and attachment, it is good also as a configuration which the configuration which considered above-mentioned both, i.e., the main frame, is equipped with said program encryption storage means, said program read-out means, said program starting means, and said program elimination means, and is equipped with said

program decryption means and said key decryption means while attachment memorizes the decryption key corresponding to said user.

[0052] Thus, if constituted, since the decryption key corresponding to a user, a program decryption means, and a key decryption means exist, all the safeties of the program of the decryption key corresponding to the user and a program decryption means and the program of a key decryption means will be secured, and the safety of data will be further secured to an attachment side.

[0053] Moreover, when said attachment did not carry out immediate memory of the decryption key but the decryption key was needed, it is good also as what generates a decryption key by the operation using Control Code. Moreover, said program is good also as what has the function to stop self processing and to perform processing of said program elimination means, when the next alter operation is not performed by the user within predetermined time. If it does in this way, even if a just user will once separate from a system unit, since the program of a plaintext condition itself disappears after a while, it is analyzed by the third person or is not altered.

[0054] Moreover, you may constitute as an information secrecy processing system combining the encryption system of one of the configurations mentioned above, and one of the decryption systems mentioned above. While it can have the function of both an encryption system and a decryption system and processing of a user becomes efficient with one information secrecy processing system by this, the safety of a program or data is also secured.

[0055] In addition, in the encryption system mentioned above, it can constitute as data telecommunication systems, such as facsimile apparatus which is equipped with a transmitting means to transmit encryption data to the other party through a communication line, for example, has an encryption function. Moreover, in the decryption system mentioned above, it can constitute similarly as data telecommunication systems, such as facsimile apparatus which is equipped with a receiving means to receive encryption data through a communication line, for example, has the decode function of encryption data.

[0056] Of course, the encryption system which has an above-mentioned transmitting means, and the decryption system which has an above-mentioned receiving means can be constituted as information secrecy communication system, such as facsimile apparatus which has combination, an encryption function, and an encryption data decode function.

[0057]

[Example] Drawing 1 and drawing 2 show one example of the information secrecy processing system of this invention. Among this, drawing 1 shows the block diagram of an information processor 2. The information processor 2 is equipped with CPU4, ROM6, RAM8, backup RAM 10, a keyboard 12, the magneto-optic-disk (MOD) drive 14, CRT display 16, hard disk (HD) equipment 18, the floppy disk (FD) drive 20, and the input/output interface (I/O) 22. These configurations are connected in signal by bus 24, and the IC card reader 26 is further connected to I/O22.

[0058] Thus, the magneto-optic disk which the information processor 2 was constituted as a computer and inserted in ROM6 and Magnetic-Optical disk drive 14, It is based on the program and data which were read from IC card 30 (drawing 2) inserted in the floppy disk or the IC card reader 26 inserted in the hard disk drive unit 18 and the floppy disk drive 20. The magneto-optic disk in which the data which performed required processing and were obtained as a result were inserted by Magnetic-Optical disk drive 14, It memorizes to IC card 30 inserted in the floppy disk or the IC card reader 26 inserted in the hard disk drive unit 18 and the floppy disk drive 20. An information processor 2 may be equipped with CD-ROM drive equipment, magnetic tape storage, etc. in addition to this.

[0059] The block diagram of IC card 30 is shown in drawing 2 . IC card 30 is equipped with CPU32, ROM34, RAM36, backup RAM 38, and an input/output interface (I/O) 40. These configurations are connected in signal by bus 42. In addition, I/O40 is the interface equipped with the connector to the IC card reader 26 of an information processor 2.

[0060] The initial program IP for enciphering and decrypting data to the program area of RAM8 by power-source ON of said information processor 2, as shown in drawing 3 (a) is loaded and started from a hard disk drive unit 18. In addition, as shown in drawing 3 (b), the 2nd dark / "decryption processing program" Pr1-Prn as which plurality was enciphered in addition to the initial program IP are stored in the hard disk drive unit 18. It will be enciphered with the encryption key (the 1st encryption key) of the user of this information processor 2, and only the number of users will exist, and these 2nd dark / "decryption processing program" Pr1-Prn(s) will be programs which have the same function fundamentally, if it decrypts. However, a function which is different for every user so that it may mention later can also be given. Correspondence with a user and a program is performed by referring to the user ID-program address table in the hard disk drive unit 18 shown in drawing 3 (b). These 2nd dark / "decryption processing program" Pr1-Prn, and user ID-program address tables are beforehand installed in the hard disk drive unit 18 with said initial program IP.

[0061] moreover, for the backup RAM 38 of IC card 30 As shown in drawing 4 , the program of password collate-program Pr11, encryption processing program Pr12, decryption processing program Pr13, key encryption processing program Pr14, and key decryption processing program Pr15 grade, A just user's password, a just user's ID, The other party encryption keys K1, K2, --, Kn corresponding to ID (ID1, ID2, --, IDn) and ID of the partner whom a just user's dark / decryption key (it corresponds to the 1st encryption key and a decryption key), and a just user permit a decryption of data are memorized.

[0062] In order that a user may encipher data, when power-source ON of the information processor 2 is carried out, the initial program IP shown in the flow chart of drawing 5 and drawing 6 is started. First, initialization processing is performed at step S100, the initial state of the various configurations which exist in an information processor 2 is set up, and processing of determining the initial value of the data used for a program is made.

[0063] Next, it is judged whether the IC card reader 26 is equipped with IC card 30 (S110). If not equipped, a negative judging is carried out at step S110, the display which requires wearing of IC card 30 is performed to CRT display 16 (S120), and the processing which performs step S110 again is repeated.

[0064] If the IC card reader 26 is equipped with IC card 30, an affirmation judging will be carried out at step S110, and the display which requires a password next will be made by CRT display 16 (S130). This password asks for the password of the just user of IC card 30 shown in drawing 4 R> 4.

[0065] If it is judged whether the input of a password was made from the keyboard 12 (S140) and there is no input, processing of steps S140 and S150 will be repeated until it is judged with a time-out at step S150. If it corresponds to a time-out, and the input of a password is not made even if it carries out predetermined time progress, at step S150, an affirmation judging is carried out and processing of this initial program is ended. If the input of a password is before carrying out a time-out, the password which the affirmation judging was carried out and was entered at step S140 will be transmitted to an IC card 30 side. And it waits to transmit the collating result and a user's ID of a password from an IC card 30 side next (S170).

[0066] The processing by the side of IC card 30 is shown in the flow chart of drawing 7 - drawing 8 . This processing is processing started when the IC card reader 26 is equipped with IC card 30. First, it becomes the receiving waiting of the password from an information processor 2 (S500). If a password is transmitted, an affirmation judging will be carried out at step S500 by processing of step S160 mentioned above, and collating with the password of the just user of this IC card 30 memorized by password collate-program Pr11 by the backup RAM 38 shown in drawing 4 and the password sent from the information processor 2 is made (S520).

[0067] And the result of the collating and a just user's ID are transmitted to an information-processor 2 side (S530). If the password of the just user by whom the collating result was memorized in "agreement" 38, i.e., the password from an information processor 2 and Backup RAM, is in agreement, since it turns out that the just user is using the IC card 30, a user's just its dark / decryption key are read from backup RAM 38 next (S550). When the collating result of a password becomes an inequality, a negative judging is carried out at step S540, and it returns to processing of step S500 again.

[0068] When step S550 is processed, it becomes the transmitting waiting from an information processor 2 next (S560). If a collating result and ID are transmitted to an information processor 2 by processing of step 530, in an information-processor 2 side, it will be judged whether the affirmation judging was carried out at step 170, and then it agreed (S180). By the just user, if it has not agreed, since there is nothing, a negative judging is carried out at step 180, if inharmonious things and processing are stopped is displayed on CRT display 16 (S190), and it returns to processing of step S110. Therefore, if the IC card reader 26 is equipped with IC card 30, again, a password will be required at step 130 and it will become the waiting for a password input in step 140 and S150. What is necessary is just to correct again, if it is a just user, since it can ask for an input even if it mistakes the input of a password. However, since, as for making a password repeat and enter, the possibility of coincidence becomes high in being unjust use, the input mistake of a password is made in to 3 times, at step S180, in the case of the 3rd mistake, it does not return to step S110, but this initial program is ended.

[0069] If a judgment that it agreed at step S180 is made, the display of the purport corresponding to CRT display 16 will be made (S200), the 2nd enciphered dark / decryption processing program corresponding to ID which received with the collating result from IC card 30 next will be discovered from the storage file of a hard disk drive unit 18, and it will transmit to an IC card 30 side (S210). As shown in drawing 3 (b), from the user ID-program address table filed by the hard disk drive unit 18, looking for a program from ID obtains the address on the disk of the 2nd enciphered dark / decryption processing program corresponding to ID, and it is performed by reading the 2nd [which corresponds from the address] enciphered dark / decryption processing program. For example, if a user's ID is IDb, it will become clear from a user ID-program address table that the 2nd enciphered dark / decryption processing program Pr2 correspond, and the 2nd enciphered dark / decryption processing program Pr2 will be read from the disk address.

[0070] Next, it becomes the transmitting waiting from IC card 30 (S220). In an IC card 30 side, if there is transmission of the 2nd dark / decryption processing program Pr2 enciphered from the information processor 2, an affirmation judging will be carried out by the judgment of step S560, and then reception and the received decryption processing of a program Pr 2 of the program Pr 2 will be made (S570). That is, decryption processing program Pr13 which exists in backup RAM 38 is started, and the program Pr 2 transmitted from the information processor 2 is decrypted. In addition, when a program Pr 2 is long and cannot transmit or decrypt at once by the relation between a buffer or activity memory space, it may divide, and you may transmit or decrypt.

[0071] Next, the 2nd decrypted dark / decryption processing program Pr2 are transmitted to an information processor 2 (S580). Next, if it is judged whether the key and the decryption candidate ID were received temporarily which has not been enciphered (S590) and it has not received, it is judged whether the key was received temporarily which was enciphered (S595). If this has not received, either, it is judged whether the 2nd dark / decryption processing program which has not been enciphered were received (S600). Before neither has received, the judgment of step S590, step S595, and step S600 is repeated.

[0072] In an information-processor 2 side, if it was decrypted, namely, the 2nd dark / decryption processing program Pr2 of a plaintext are received from an IC card 30 side, an affirmation judging will be carried out at step S220, and the 2nd dark / decryption processing program Pr2 of the plaintext will be transmitted to activity memory area PA of RAM8, as shown in drawing 2 (a) (S230).

[0073] Next, the 2nd dark / decryption processing program Pr2 of this plaintext are started from an initial program (S240). The flow chart of the 2nd its dark / decryption processing program Pr2 is shown in drawing 9 - drawing 12 . This processing is performed by starting processing of step S240.

[0074] Initiation of processing of the 2nd dark / decryption processing program Pr2 displays a processing menu on CRT display 16 first (S1010). Menus are encryption processing (S1100), decryption processing (S1200), modification processing (S1300) of the 2nd dark / decryption processing program, and other processings (S1400).

[0075] Here, a user's selection of encryption processing (S1100) starts the processing shown in drawing 10 . First, the input of the data name for encryption and the decryption candidate ID is required (S1102). The data name for encryption is performed by specifying the file in the floppy disk set to the magneto-optic disk, the hard disk drive unit 18, or floppy disk drive 20 set to Magnetic-Optical disk drive 14. Here, since encryption data are stored in a magneto-optic disk, the data for encryption shall exist in a floppy disk.

[0076] Moreover, the decryption candidate ID inputs ID of the partner who permits a decryption. If the other party who permits a decryption is plurality, two or more ID will be inputted. In addition, if a group's ID registered beforehand is inputted, it means specifying ID of two or more partners belonging to the group, and two or more persons can be made into a decryption candidate by one ID.

[0077] It becomes the waiting for an input until predetermined time-out time amount passes in time out treatment (S1106) here (S1104). To a time-out, if there is no input, an affirmation judging will be carried out at step S1106, and it will return to an initial program immediately, but if the input of the data name for encryption and the decryption candidate ID is made, a key (the 2nd encryption key) will be generated next temporarily (S1108).

[0078] Here, as for generation of a key, it is desirable that it is a different key (a value and character string) for every generation temporarily. For example, the approach of measuring the time interval of the approach by the M sequence random-number-generation program or a key stroke in about 1/100,000 second, and taking out only a low-ranking need digit count etc. is mentioned. In this way, it becomes the receiving waiting of a key temporarily [which was enciphered] which transmits a key and the decryption candidate ID to an IC card 30 side temporarily which was generated (S1110), and then is transmitted from an IC card 30 side (S1120).

[0079] In an IC card 30 side, since the key and the decryption candidate ID were received temporarily, an affirmation judging is carried out at step S590 of drawing 8 , next a key is enciphered temporarily with the other party encryption key corresponding to the decryption candidate ID by key encryption processing program Pr14 (S610). In the backup RAM 38 of

IC card 30 From the other party encryption keys K1, K2, --, Kn corresponding to ID1, ID2, --, IDn, and its ID of the partner whom a just user permits a decryption of data being memorized as shown in drawing 4 For example, if the decryption candidate ID is ID2, the corresponding other party encryption key K2 will be chosen, and a key will be enciphered with the other party encryption key K2 temporarily. Moreover, as long as a group's ID is inputted, an other party encryption key may be chosen from ID of those who become the group's representation, and a key may be enciphered with the other party encryption key temporarily, and a key may be enciphered with a group's original other party encryption key temporarily.

[0080] Next, a key is transmitted to an information-processor 2 side temporarily which was enciphered in this way (S620), and processing with IC card 30 returns to processing of step S500. In an information-processor 2 side, since the key was received temporarily which was enciphered, a key is stored in a storage as a file with ID temporarily which the affirmation judging was carried out and was enciphered at step S1120 (S1130). Although this storage is a storage specified by a user, it is the magneto-optic disk set to Magnetic-Optical disk drive 14 here. Of course, the storage of floppy disk or hard disk drive unit 18 and others may be used.

[0081] Next, the data for encryption is enciphered temporarily which the data for encryption already inputted at step S1102 are read (S1140), and is not enciphered with a key, i.e., a one time [being generated at step S1108] key, (S1150). As a program which carries out encryption processing of such data using a key, DES which is a U.S. standard algorithm, FEEL to which NTT developed are known.

[0082] Next, this enciphered data is stored in the file stored in the key ID and temporarily enciphered (S1160). That is, as shown in drawing 13 , it stores as a header a decode person's (those who permit decode) ID (1), ID (2), --, temporarily [encryption] corresponding to ID (n) and its ID as key K (1), K (2), --, a file that indicated the encryption data enciphered with the key as data division temporarily by indicating a list with K (n).

[0083] In this way, encryption processing (S1100) is completed with an information processor 2, and when the data [say / the data for encryption of being read by the activity memory area of RAM8 by processing of step S1140 on RAM8] which are not enciphered next exist, processing (S1500) which clears the data is performed.

[0084] In this way, the 2nd dark / decryption processing are completed, and it returns to an initial program. In an initial program, processing of step S250 shown in drawing 6 is performed, the 2nd dark / decryption processing program which exists on RAM8 are cleared, and it returns to processing of step S110.

[0085] Thus, a data encryption is completed. As mentioned above, the program for encryption processing (drawing 9 , drawing 10) started with the information processor 2 of this example is memorized in the condition of having been enciphered by the hard disk drive unit 18, when not used for encryption processing. Therefore, since it cannot analyze and analyze by the third person, an alteration is also impossible.

[0086] When a just user enciphers data, by reading said program enciphered with a just user's dark / decryption key from a hard disk drive unit 18, decrypting the program with a just user's dark / decryption key, and starting the decrypted program, the data for encryption can be made to be able to encipher with a key (the 2nd encryption key) temporarily, and it can consider as encryption data.

[0087] And after a data encryption is completed, the started program is eliminated. For this reason, without the program for encryption of a plaintext condition remaining, even after carrying out encryption processing, the safety of the program for encryption is secured and the safety of the enciphered data is also secured as a result. Therefore, it is not necessary to take out the storage which has memorized the program for encryption processing from a storage

area for every encryption processing, and to do the activity set and loaded to an information processor 2, and an encryption activity can be performed efficiently.

[0088] Moreover, since it is cleared when the data before encryption also remain on the activity memory area, safety is more high. Furthermore, a key (the 2nd encryption key) is enciphered with an other party encryption key (the 3rd encryption key) temporarily. And a key is contained by encryption data and one file with ID of those who permit a decryption temporarily [this] that was enciphered.

[0089] Thus, since the momentary key (the 2nd encryption key) for enciphering data is further enciphered with the other party encryption key (the 3rd encryption key), insurance is securable even if it adds the key (the 2nd encryption key) to encryption data temporarily. Moreover, since a key (the 2nd encryption key) is added to encryption data temporarily, encryption data can be decrypted, if even the other party encryption key (the 3rd encryption key) is kept at a carrying place or the communications-partner point even if it transmits carrying with the storage (here magneto-optic disk) ****, or its encryption data to the other party by communication link.

[0090] A key (the 2nd encryption key) is called for by the operation by the program for said encryption temporarily. Thus, the encryption key for enciphering data is a temporary key only for the encryption at that time, and since it is not used continuously, the safety of data is secured more. Moreover, since it is calculating within the program for said encryption and only what that program was enciphered as exists except the time of encryption processing, a third person cannot alter a key temporarily [this], either, so that the key which he knows may be generated.

[0091] The information secrecy processing system of this example Moreover, the information processor 2 as the main frame, It is separated and constituted by IC card 30 as attachment [this information processor 2] which it is constituted by another object, and it connects with arbitration in signal, or can be cut to an information processor 2. An information processor 2 And program encryption storage processing, program read-out processing, While it has each program of program starting processing and program elimination processing and IC card 30 memorizes a just user's dark / decryption key, and other party encryption key (3rd encryption key) It considers as the configuration equipped with each program of program decryption processing and key encryption processing. That is, since the program of a user's just dark / decryption key, an other party encryption key (the 3rd encryption key), and program decryption processing and the program of key encryption processing exist, the safety of the program of a user's just its dark / decryption key, an other party encryption key (the 3rd encryption key), and program decryption processing and the program of key encryption processing is secured, and the safety of data is further secured to an IC card 30 side.

[0092] Next, when the magneto-optic disk which stored the encryption data file shown in drawing 13 is received, the processing which decrypts the data is explained. First, after an information processor 2 carries out power-source ON, a user sets the received magneto-optic disk to Magnetic-Optical disk drive 14, and sets self IC card 30 to the IC card reader 26.

[0093] An initial program is started in an information processor 2. The processing in this case is as having explained step S240 from step S100 on the occasion of data encryption. Also in IC card 30, it is the same. Of course, if users differ, since IC cards 30 also differ, ID which receives at step S170 also differs, and dark differs also from the 2nd [which is transmitted to IC card 30 at step S210] enciphered decryption processing program.

[0094] For example, if a user's ID is IDa, as for the program by which it is transmitted to IC card 30, consequently the 2nd enciphered dark / decryption processing program Pr1 are started by step S240 from the 2nd enciphered dark / decryption processing program Pr1

corresponding, the 2nd dark / decryption processing program Pr1 will be performed. In addition, it is explained here that the 2nd dark / decryption processing program Pr1 are the same contents as the 2nd dark / decryption processing program Pr2.

[0095] If the 2nd dark / decryption processing program Pr1 are started at step S240, the display of a processing menu will be first made at step S1010 of the flow chart shown in drawing 9 . If a user chooses decryption processing here, processing of step S1200 will be started. This decryption processing is shown in the flow chart of drawing 11 .

[0096] First, the demand of the data name input for a decryption is displayed (S1202). Next, it becomes the input waiting (S1204) until it is judged with a time-out at step S1206. If it becomes a time-out, without making an input, an affirmation judging will be carried out at step S1206, the 2nd dark / decryption processing are ended, and it returns to an initial program.

[0097] When one data file in the magneto-optic disk set to Magnetic-Optical disk drive 14 is specified (all the files in a magneto-optic disk may be specified, and) all the files in a specific directory may be specified. An affirmation judging is carried out at step S1204, and key K (1), K (2), and -- are read from the header of the encryption data for [the] a decryption the decryption candidates ID (1) and ID (2), --, temporarily [corresponding] that was enciphered (S1208).

[0098] Next, it is judged whether a user's ID exists in these decryption candidates ID (1) and ID (2) and -- (S1210). That is, it is judged whether a user's ID indicated by IC card 30 set to the IC card reader 26 is specified as a decryption candidate. If it does not exist, since the decryption is not permitted, the negative judging of the just user of IC card 30 by which the current set is carried out is carried out at step S1210, and a decryption displays that it is disapproval on CRT display 16 (S1220), ends the 2nd dark / decryption processing, and returns to an initial program. In addition, if at least one file with which a user's ID indicated by IC card 30 is specified as the header as a decryption candidate exists when multiple files are directed as a candidate for a decryption, processing after step S1230 will be performed only about the file included. Moreover, if the just user of IC card 30 is contained in the group when a group's ID is specified as the header, the just user will presuppose that it is specified as the header.

[0099] If ID (1) corresponds when a just user's ID indicated by IC card 30 is contained in the decryption candidates ID (1) and ID (2) and -- for example An affirmation judging is carried out at step S1210, key K (1) is transmitted to an IC card 30 side temporarily [which was enciphered] which was read from the header of the file for a decryption (S1230), and it becomes the receiving waiting (S1240) of a key temporarily which was decrypted next.

[0100] If key K (1) is received temporarily which was enciphered in the condition of having repeated steps S590, S595, and S600 in the IC card 30 side, an affirmation judging will be carried out at step S595, and key K (1) will be decrypted temporarily temporarily which was enciphered by key decryption processing program Pr15 with dark / decryption key of the just user who has memorized to backup RAM 38 (S630).

[0101] Next, a key is transmitted to an information processor 2 temporarily which was decrypted (S640), and it returns to processing of step S500. In an information-processor 2 side, since the key was received temporarily which was decrypted, an affirmation judging is carried out at step S1240, and it decrypts with a key temporarily which had the data division of the data for a decryption decrypted, and stores in a storage (S1250).

[0102] In this way, after decryption processing (S1200) is completed, when the data which are not enciphered on RAM8 at step S1500 mentioned above, i.e., the decrypted data, exist, processing which clears the data is performed. In this way, the 2nd dark / decryption

processing are completed, and it returns to an initial program. In an initial program, processing of step S250 shown in drawing 6 is performed, the 2nd dark / decryption processing program which exists on RAM8 are cleared, and it returns to processing of step S110.

[0103] Thus, a decryption of data is completed. As mentioned above, the program for decryption processing (drawing 9 , drawing 11) started with the information processor 2 of this example is memorized in the condition of having been enciphered by the hard disk drive unit 18, when not used for decryption processing. Therefore, since it cannot analyze and analyze by the third person, an alteration is also impossible.

[0104] It is a key (it corresponds to the 2nd decryption key.) about encryption data temporarily by reading said program enciphered with a just user's dark / decryption key from a hard disk drive unit 18, decrypting the program with a just user's dark / decryption key, and starting the decrypted program, when a just user decrypts decryption data. That is, there is a key also with the 2nd encryption key and it is also the 2nd decryption key temporarily. It can be made to be able to decrypt and can carry out to decryption data, i.e., plaintext data.

[0105] And after a decryption of encryption data is completed, the started program is eliminated. For this reason, without the program for a decryption of a plaintext condition remaining, even after carrying out decryption processing, the safety of the program for a decryption is secured and the safety of data is also secured as a result. Therefore, it is not necessary to take out the storage which has memorized the program for decryption processing from a storage area for every decryption processing, and to do the activity set and loaded to an information processor 2, and a decryption can be done efficiently.

[0106] Moreover, since it is cleared when the decrypted data also remain on the activity memory area, safety is more high. Furthermore, a key (the 2nd decryption key) is decrypted with a just user's dark / decryption key temporarily [which was enciphered] which is contained in encryption data.

[0107] By doing in this way, the momentary key (the 2nd decryption key) for decrypting encryption data is obtained, and only a just user can decrypt encryption data appropriately and can get plaintext data. It separates to IC card 30 as attachment [the information processor 2 as the main frame, and this information processor 2] which it is constituted by another object, and it connects with arbitration in signal, or can be cut to an information processor 2, and this examples are consisted of. Moreover, an information processor 2 While it has each program of program encryption storage processing, program read-out processing, program starting processing, and program elimination processing and IC card 30 memorizes a just user's dark / decryption key It considers as the configuration equipped with the program of program decryption processing and key decryption processing.

[0108] Thus, since it is constituted, since the program of a user's just dark / decryption key, program decryption processing, and key decryption processing exists, the safety of the program of the dark / decryption key corresponding to the just user, and program decryption processing and the program of key decryption processing is secured, and the safety of data is further secured to an IC card 30 side.

[0109] Next, modification processing of the 2nd enciphered dark decryption processing program which is memorized by the hard disk drive unit 18 is explained. First, after an information processor 2 carries out power-source ON, a user sets the received magneto-optic disk to Magnetic-Optical disk drive 14, and sets self IC card 30 to the IC card reader 26.

[0110] An initial program is started in an information processor 2. The processing in this case is as having explained step S240 from step S100 on the occasion of data encryption or a decryption. Also in IC card 30, it is the same. Of course, if users differ, since IC cards 30 also

differ, ID which receives at step S170 also differs, and dark differs also from the 2nd [which is transmitted to IC card 30 at step S210] enciphered decryption processing program.

[0111] For example, if a user's ID is IDc, as for the program by which it is transmitted to IC card 30, consequently the 2nd enciphered dark / decryption processing program Pr3 are started by step S240 from the 2nd enciphered dark / decryption processing program Pr3 corresponding, the 2nd dark / decryption processing program Pr3 will be performed. If the 2nd dark / decryption processing program Pr3 are started at step S240, the display of a processing menu will be first made at step S1010 of the flow chart shown in drawing 9 .

[0112] If a user chooses program modification processing here, processing of step S1300 will be started. Program modification processing is shown in the flow chart of drawing 12 . First, edit processing of the 2nd dark / decryption processing program is made (S1302). For example, the 2nd dark / decryption processing program currently expressed in hexadecimals are disassembled, it expresses in assembly language, and edit by the keyboard 12 is enabled. If edit is completed, the contents after edit will be assembled and it will be changed into the program which can be performed.

[0113] In addition, in this edit processing, the processing replaced with other already changed [only] programs is also included. Therefore, the program created with other equipments can newly be incorporated as the 2nd dark / decryption processing program. Moreover, in this edit processing, modification of data, such as a numeric value only set up into the program and a character string, is also included.

[0114] Next, the 2nd dark / decryption processing program after edit are transmitted to an IC card 30 side (S1304), and it becomes the receiving waiting (S1306) of the 2nd enciphered dark / decryption processing program. In the condition of having repeated steps S590, S595, and S600 in the IC card 30 side, if the 2nd dark / decryption processing program which has not been enciphered are received, an affirmation judging will be carried out at step S600, and the 2nd dark / decryption processing program will be enciphered program encryption processing program Pr12 with dark / decryption key of the just user of IC card 30 (S650).

[0115] Next, this the 2nd enciphered dark / decryption processing program are transmitted to an information processor 2 (S660), and it returns to processing of step S500. In an information-processor 2 side, since the 2nd enciphered dark / decryption processing program were received, an affirmation judging is carried out at step S1306, the 2nd dark / decryption processing program enciphered next are contained to a hard disk drive unit 18, and the disk address is entered in the program address Pr 3 to which it was made to correspond as IDc among user ID-program address tables (S1308).

[0116] In this way, program modification processing is ended. Henceforth, step S1500 is processed and it returns to an initial program. In an initial program, processing of step S250 is performed, the 2nd dark / decryption processing program which exists on RAM8 are cleared, and it returns to processing of step S110.

[0117] As mentioned above, since the program modification processing (drawing 9 , drawing 12) started with the information processor 2 of this example can change the contents of the 2nd dark / decryption processing program with which it was enciphered only for the users by the just user, it becomes possible [dark/decrypting] with a different algorithm for every user of the, or the different set point (when the data in a program are changed).

[0118] Therefore, also when changing the program for every user and one person's dark / decryption algorithm are analyzed by the third person, it is not analyzed by coincidence to all the members' program. Moreover, by program modification processing, when analyzed, when a just user changes a program, safety can be secured about future information.

[0119] Moreover, in this example, even if it leaves an information processor 2 as a user is processing since the 2nd dark / decryption processing program which the 2nd dark / decryption processing program are ended by time out treatment (S1106, S1206), and processing of step S250 ** is performed, and exists on RAM8 are cleared when alter operation is not performed, the analysis and the alteration by the third person can be prevented. As long as actuation is no longer performed in the middle of edit also at step S1302, the 2nd dark / decryption processing program may be ended.

[0120] Moreover, in an information-processor 2 side, since the data encryption for [of the amount of data / large] encryption or decryption processing is performed and encryption or decryption processing of a key is performed in an IC card 30 side the small program of the amount of data, and temporarily, as the whole processing, it can carry out to a high speed. Moreover, it can consider as a configuration small as IC card 30, and cheap.

[0121] Moreover, as shown in drawing 13 , only a key is enciphered temporarily corresponding to the number of those who permit a decryption, and even if the amount of data which keeps, carries or communicates from one actual encryption data existing has many those who permit a decryption, it does not turn into a huge day large quantity, but can save memory, a storage, or communication link time amount.

[0122] In this example, a hard disk drive unit 18 corresponds to a program encryption storage means. Step S210 corresponds to the processing as a program read-out means, and step S570 corresponds to the processing as a program decryption means. Step S240 corresponds to the processing as a program starting means, and step S250 corresponds to the processing as a program elimination means. Step S610 corresponds to the processing as a key encryption means, step S1160 corresponds to the processing as a key addition means, and step S630 corresponds to the processing as a key decryption means.

[0123] Although the example which carried out [other] **** was an information secrecy processing system which decrypts the data which enciphered data or were enciphered and is returned to plaintext data Furthermore, when an information processor 2 is equipped with a network control unit and a modem Like said example, a just user enciphers data and transmits to the other party through a communication line. Moreover, you may constitute as information secrecy communication system which a user (decryption candidate) just like said example decrypts the encryption data which the other party has transmitted through a communication line, and obtains them as plaintext data.

[0124] Furthermore, by having the image reader of a manuscript, and the recording apparatus of an image, it constitutes in this information secrecy communication system as facsimile apparatus, and is good for it also as an object of encryption or a decryption like said example in the image data of that manuscript. Although the just user and the decryption candidate were specified by ID in said example, it may not be ID, or a candidate name is sufficient, and both ID and a candidate name are sufficient.

[0125] Although a just user's dark / decryption key memorized by IC card 30 were used for encryption and a decryption in said example, at the time of a decryption, a private key may be used using a public key at the time of encryption. Therefore, the other party encryption keys K1, K2, --, Kn with which a just user permits a decryption of data may be public keys.

[0126] Moreover, although ID1 and ID2 of the other party who permits a decryption, --, the encryption keys K1 and K2 corresponding to it and -- were memorized by the backup RAM 38 of IC card 30, direct, such ID, and the encryption key K may not be memorized, but you may make it be a degree.

[0127] That is, when ID of the other party who builds a secret algorithm in backup RAM 38, and permits a decryption is inputted, it is good also as a configuration which generates the

encryption key K which corresponds in data processing according to the algorithm. It becomes saving of memory when there are much those who permit a decryption, since an encryption key can be obtained from much ID only with one algorithm even if it does not memorize two or more encryption keys if it is made this configuration.

[0128] The configuration which generates a key is applied from this ID also to dark / decryption key of the just user of IC card 30 by data processing, and you may make it generate dark / decryption key from a just user's ID. Moreover, since a program, each key, etc. are kept to backup RAM 38 and a program, a key, etc. will be eliminated if the switch which is interlocked with sheathing and becomes off at the time of sheathing disconnection is used between a backup power supply and backup RAM 38, and sheathing is opened, IC card 30 is more desirable on insurance. Moreover, a program, a key, etc. may be memorized to EEPROM instead of backup RAM 38. In this case, if the switch which is interlocked with sheathing and serves as ON at the time of sheathing disconnection is formed between a power source and EEPROM, and sheathing is opened, a current will flow and a program, a key, etc. will be eliminated.

[0129] The initial program may be stored in ROM6 instead of a hard disk drive unit 18 in said example.

CLAIMS

[Claim(s)]

[Claim 1] In the encryption system which enciphers data by encryption processing based on a program A program encryption storage means to memorize said program in the condition of having enciphered with the 1st encryption key corresponding to a user, The program read-out means which reads said program enciphered with the 1st encryption key corresponding to a user from the inside of said program encryption storage means, By starting the program decrypted by program decryption means to decrypt said program read by said program read-out means with the decryption key corresponding to a user, and said program decryption means The program starting means which is made to encipher the data for encryption with the 2nd encryption key, and is used as encryption data, The encryption system characterized by having a program elimination means to eliminate said program which was decoded and became a candidate for starting when the data encryption for encryption was completed with said program starting means.

[Claim 2] Furthermore, the encryption system [equipped with a key encryption means to encipher said 2nd encryption key with the 3rd encryption key, and a key addition means to add said 2nd encryption key enciphered with said key encryption means to said encryption data] according to claim 1.

[Claim 3] The encryption system according to claim 2 with which said key addition means is realized as a function of said program.

[Claim 4] The encryption system according to claim 1 to 3 with which said program asks for the 2nd encryption key by the operation.

[Claim 5] The main frame and this main frame are the encryption system according to claim 1 with which it consists of attachment which it is constituted by another object, and it connects with arbitration in signal, or can be cut to said main frame, and said main frame is equipped with said program encryption storage means, said program read-out means, said program starting means, and said program elimination means, and it is equipped with said program

decryption means while said attachment memorizes the decryption key corresponding to said user.

[Claim 6] It consists of attachment [the main frame and this main frame] which it is constituted by another object, and it connects with arbitration in signal, or can be cut to said main frame. Said main frame Said program encryption storage means, said program read-out means, The encryption system according to claim 3 with which it has said program decryption means, said program starting means, and said program elimination means, and it is equipped with said key encryption means while said attachment memorizes said 3rd encryption key.

[Claim 7] It consists of attachment [the main frame and this main frame] which it is constituted by another object, and it connects with arbitration in signal, or can be cut to said main frame. Said main frame Said program encryption storage means, said program read-out means, The encryption system according to claim 3 with which it has said program starting means and said program elimination means, and it is equipped with said program decryption means and said key encryption means while said attachment memorizes the decryption key corresponding to said user, and said 3rd encryption key.

[Claim 8] The encryption system according to claim 6 or 7 which said attachment memorizes as a list with which the decryption was corresponded in said 3rd encryption key with a person's Control Code to permit.

[Claim 9] The encryption system according to claim 5 to 7 which generates said decryption key or said 3rd encryption key by the operation using Control Code when said attachment did not carry out immediate memory of said decryption key or said 3rd encryption key but said decryption key or said 3rd encryption key was needed.

[Claim 10] The encryption system according to claim 1 to 9 with which said program has the function to stop self processing and to perform processing of said program elimination means when the next alter operation is not performed by the user within predetermined time.

[Claim 11] In the decryption system which decrypts encryption data by decryption processing based on a program A program encryption storage means to memorize said program in the condition of having enciphered with the 1st encryption key corresponding to a user, The program read-out means which reads said program enciphered with the 1st encryption key corresponding to a user from the inside of said program encryption storage means, By starting said program decrypted by program decryption means to decrypt said program read by said program read-out means with the decryption key corresponding to a user, and said program decryption means The program starting means which is made to decrypt encryption data with the 2nd decryption key, and is used as decryption data, The decryption system characterized by having a program elimination means to eliminate said program which was decrypted and became a candidate for starting when the decryption of encryption data was completed with said program starting means.

[Claim 12] Furthermore, the decryption system [equipped with a key decryption means to decrypt the enciphered 2nd decryption key which is contained in said encryption data with the decryption key corresponding to a user] according to claim 11.

[Claim 13] The main frame and this main frame are the decryption system according to claim 11 by which it consists of attachment which it is constituted by another object, and it connects with arbitration in signal, or can be cut to said main frame, and said main frame is equipped with said program encryption storage means, said program read-out means, said program starting means, and said program elimination means, and it is equipped with said program decryption means while said attachment memorizes the decryption key corresponding to said user.

[Claim 14] It consists of attachment [the main frame and this main frame] which it is constituted by another object, and it connects with arbitration in signal, or can be cut to said main frame. Said main frame Said program encryption storage means, said program read-out means, The decryption system according to claim 12 by which it has said program decryption means, said program starting means, and said program elimination means, and it is equipped with said key decryption means while said attachment memorizes the decryption key corresponding to said user.

[Claim 15] It consists of attachment [the main frame and this main frame] which it is constituted by another object, and it connects with arbitration in signal, or can be cut to said main frame. While it has said program encryption storage means, said program read-out means, said program starting means, and said program elimination means and said attachment memorizes the decryption key corresponding to said user, said main frame A decryption system [equipped with said program decryption means and said key decryption means] according to claim 12.

[Claim 16] The decryption system according to claim 13 to 15 which generates said decryption key by the operation using Control Code when said attachment did not carry out immediate memory of said decryption key but said decryption key was needed.

[Claim 17] The decryption system according to claim 11 to 16 by which said program has the function to stop self processing and to perform processing of said program elimination means when the next alter operation is not performed by the user within predetermined time.

[Claim 18] Claims 1-10 are the information secrecy processing systems with which it comes to put the encryption system and the decryption system according to claim 11 to 17 of a publication together either.

[Claim 19] Claims 1-10 equipped with a transmitting means to transmit said encryption data to the other party through a communication line are the encryption systems of a publication either.

[Claim 20] Claims 11-17 equipped with a receiving means to receive said encryption data through a communication line are the decryption systems of a publication either.

[Claim 21] Information secrecy communication system with which it comes to put an encryption system and a decryption system according to claim 20 according to claim 19 together.